(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
12 September 2003 (12.09.2003)

PCT

(10) International Publication Number
WO 03/075125 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number: PCT/US03/06169

(22) International Filing Date: 28 February 2003 (28.02.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/361,419	1 March 2002 (01.03.2002)	US
60/361,421	1 March 2002 (01.03.2002)	US
60/361,420	1 March 2002 (01.03.2002)	US
60/361,380	1 March 2002 (01.03.2002)	US
60/387,331	10 June 2002 (10.06.2002)	US
60/387,330	10 June 2002 (10.06.2002)	US

(71) Applicant *(for all designated States except US)*: ENTERASYS NETWORKS, INC. [US/US]; 50 Minuteman Road, Andover, MA 01810 (US).

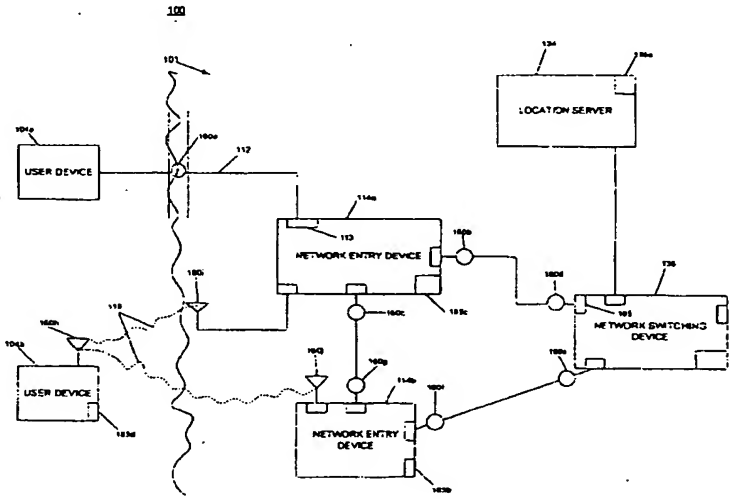
(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: ROESE, John, J. [US/US]; 21 Moody Point Drive, Newmarket, NH 03857 (US). GRAHAM, Richard, W. [US/US]; 186 Island Pond Road, Derry, NH 03038 (US). GORSKY, John-Paul [US/US]; 5 Concord Way, Rochester, NH 03867 (US). HARRINGTON, David [US/US]; 50 Harding Road, Portsmouth, NH 03801 (US). FRATTURA, David [US/US]; 50 Minuteman Road, Andover, MA 01810 (US). DURAND, Roger, P. [US/US]; 18 Williamsburg Drive, Amherst, NH 03031 (US). FEE, Brendan, J. [US/US]; 34 Pemberton Road, Nashua, NH 03063 (US). ALLEN, Anja, A. [DE/US]; 12806 Dogwood Hills Lane, Fairfax, VA 22033 (US).

(74) Agent: ROHLICEK, J., Robin; Fish & Richardson P.C., 225 Franklin Street, Boston, MA 02110 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG,

[Continued on next page]

(54) Title: LOCATION AWARE DATA NETWORK



(57) Abstract: A system that associates physical locations with network-linked devices in a network to which such devices are connected. This system employs a variety of techniques for establishing device location. The system configuration can vary and can include any type of data network, including LANs, MANs, Wide Area Networks (WANs), Personal Area Networks (PANs), and Home Networks. The system provides location information for particular devices to the network devices and management, and may be used in any of a variety of ways to improve configuration accuracy, control, and security. The location information may also be used to control or secure a device itself.

WO 03/075125 A2

SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZM, ZW.

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

Location Aware Data Network

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims priority to the following U.S. Provisional Patent Applications: Serial No. 60/361,419, titled "A System for Network Definition Based on Device Location", filed on March 1, 2002; Serial No. 60/361,421, titled "A System to Regulate Access as a Function of Device Location", filed on March 1, 2002; Serial No. 60/361,420, titled "Systems and Methods to Define Location of a Network Device or a Networked Device", filed on March 1, 2002; Serial No. 60/361,380, titled "A System and Method to Provide Security in a Network Based on Device Location Information", filed on March 1, 2002; Serial No. 60/387,331, titled "Location Discovery and Configuration Provisioning Server", filed on June 10, 2002; and Serial No. 60/387,330, titled "System and Method for Switch Based Location Discovery and Configuration Provisioning of Network Attached Devices", filed on June 10, 2002. The entire contents of each of these applications are hereby incorporated by reference.

TECHNICAL FIELD

This description relates to determination and use of location information within a data network.

BACKGROUND

Computing systems are useful tools for the exchange of information among individuals. The information may include, but is not limited to, data, voice, graphics, and video. The exchange is established through interconnections linking the computing systems together in a way that permits the transfer of electronic signals that represent the information. The interconnections may be either cable or wireless. Cable connections include, for example, metal and optical fiber elements. Wireless connections include, for example infrared, acoustic, and radio wave transmissions.

Interconnected computing systems having some sort of commonality are represented as a network. For example, individuals associated with a college campus may each have a computing device. In addition, there may be shared printers and remotely located application servers

sprinkled throughout the campus. There is commonality among the individuals in that they all are associated with the college in some way. The same can be said for individuals and their computing arrangements in other environments including, for example, healthcare facilities, manufacturing sites and Internet access users. A network permits communication or signal exchange among the various computing systems of the common group in some selectable way. The interconnection of those computing systems, as well as the devices that regulate and facilitate the exchange among the systems, represent a network. Further, networks may be interconnected together to establish internetworks.

The process by which the various computing systems of a network or internetwork communicate is generally regulated by agreed-upon signal exchange standards and protocols embodied in network interface cards or circuitry. Such standards and protocols were borne out of the need and desire to provide interoperability among the array of computing systems available from a plurality of suppliers. Two organizations that have been responsible for signal exchange standardization are the Institute of Electrical and Electronic Engineers (IEEE) and the Internet Engineering Task Force (IETF). In particular, the IEEE standards for internetwork operability have been established, or are in the process of being established, under the purview of the IEEE 802 committee on Local Area Networks (LANs) and Metropolitan Area Networks (MANs).

SUMMARY

In a general aspect, the invention features a system that associates physical locations with network-linked devices in a network to which such devices are connected. This system employs a variety of techniques for establishing device location. The system configuration can vary and can include any type of data network, including LANs, MANs, Wide Area Networks (WANs), Personal Area Networks (PANs), and Home Networks. The system provides location information for particular devices to the network devices and management, and may be used in any of a variety of ways to improve configuration accuracy, control, and security. The location information may also be used to control or secure a device itself.

Further features relate to mechanisms by which a network entry device and/or an intermediate device acquires location information. Those mechanisms include, generally, techniques for acquiring absolute and relative location information. Absolute location

information may be obtained using known geographical identifiers in a coordinate system, such as latitude and longitude, dead reckoning, Global Satellite Positioning (GPS) systems affixed to or proximate to the device to be located, inertial locators, optical locators, and other techniques. Relative location may be obtained by vectoring from equipment having a known location, or by vectoring from a known location. Relative location also may be obtained from triangulation from known radio-based or optical-based locations, by phased array searches to define a range of locations, or by signal strength attenuation mapped to a range of locations. Other techniques may be employed to fix the position of a device of interest.

The device can determine its own position and relay that information to applications within the network at start-up, upon connection, or when queried, or the system can determine the location of the device and store that information and give it to the device if appropriate and useful. Both absolute and relative location information can also include a level of trust parameter to determine whether the location information is reliable and can be trusted by the system. Once that device location is fixed, by absolute or relative means, and associated with the device in an identifiable way, such as a file or program argument, the device location can be used in any number of ways to enhance the operation of, and services provided by, the system. For example, anywhere user credentials are required, the location of a device can be required. In other words, the location of a device becomes part of the required credentials.

In one aspect there is a method of determining a physical location of a client in a data communication network. The method includes determining an identifier of a connection point through which the client communicates with the data network and determining a physical location of the client based on the determined identifier of the connection point, including accessing a stored association between the connection point identifier and the physical location.

In other examples the method can include one or more of the following features.

The connection point can provide a communication path to the client via a cable-based transmission medium. The cable-based transmission medium can include, for example, a wire conductor or an optical fiber.

The method can also include determining a physical location in response to the client connecting to the connection point. The physical location can also be determined in response to one or more of a variety of events, such as a timer expiring, a communication link being broken, a communication session terminating, a change in a user's credential, triggering of a firewall

alarm, a new network device joining the network, prompting by a management station, particular movement of a device is detected, a shadow (users or devices of network) device is detected.

The method can further include storing associations of connection point identifiers with respective physical locations, including storing the association between the connection point identifier and the physical location prior to the client connecting to the connection point.

The method also can further include transmitting connection information from a network device, where determining the connection point identifier further comprises determining the connection point identifier using the connection information.

The method can further include determining a first portion of the connection information that identifies the network device. This first portion can include an address of the network device, such as a MAC address of the device or an IP address of the device.

The method can further include determining a second portion of the connection information that identifies a connection port of the network device that provides a communication path to the connection point. The second portion can include, for example, a MAC address of the connection port, or an index attribute contained in the device ID.

The method also can further include receiving a signal from the client and measuring, by a network device, a first characteristic of the signal. The method can further include determining the physical location based on the first characteristic. The method can further include storing associations of previously measured characteristics with respective physical locations and determining the physical location based on the first characteristic and the previously measured characteristics. The method can further include measuring, by a first network device, the first characteristic of the signal received via a cable-based transmission medium and measuring, by a second network device, a second characteristic of a signal received via a wireless transmission medium. In this example, determining the physical location can further include determining the physical location based on the measured first characteristic and the second measured characteristic.

The method can further include storing the association between the connection point identifier and the physical location using a physical location database. The method can further include storing the association between the connection point identifier and the physical location in a centralized physical location server. The method can further include storing the association between the connection point identifier and the physical location distributed among network

devices. The connection point can include a jack. The method can further include storing an association between the physical location and at least one of a MAC address, an address, a phone number, a protocol type, an asset ID, and an owner.

The method also can further include determining authentication based on the physical location. The method can further include determining a level of service based on the physical location. The method can further include employing a security feature based on physical location. The method can further include employing further comprises encrypting transmitted data based on physical location. The method can further include employing a temporary key associated with the physical location. The method can further include searching stored associations for the connection point identifier and identifying the physical location associated with the connection point identifier in the stored associations. The physical location can include a latitude and longitude format, a latitude, longitude, altitude, and accuracy format, a location identification number, a textual string representation, and/or a relative physical location with relationship information.

The method can further include establishing a connection policy based on the physical location. The method can further include authenticating a user at a network entry device based on the connection policy. The method can further include transmitting the physical location to a device associated with the connection point. The method can further include transmitting configuration information to a device associated with the connection point based on the physical location. The method can further include determining, by a trusted device, the physical location based on the connection point. The trusted device can be located within a network infrastructure. The method can further include storing an association between the physical location and a trust level. The method can further include determining the trust level of the physical location based on a device that determines the physical location.

In another aspect there is a method for surveying a data network infrastructure including a plurality of connection points. The method includes determining a physical location for a first connection point, providing to the network infrastructure the physical location for the first connection point and determining a physical location for a second connection point. The method also includes providing to the network infrastructure the physical location for the second connection point. In other examples, the method can include the following features. The method can further include storing a first association between the first connection point and its physical

location and storing a second association between the second connection point and its physical location. The method can further include identifying the first and second connection points with respective first and second connection point identifiers. The method can further include connecting a location sensing device to the first connection point. The location sensing device can include, for example, a GPS receiver, or an inertial positioning system.

In another aspect, there is a method of determining a physical location of a client in a data communication network. The method includes connecting the client to a connection point via a cable-based transmission medium and determining the connection point with which the client communicates. The method also includes determining a physical location of the client based on the connection point and storing an association between the connection point and the physical location.

In another aspect, there is a system including a location module configured to determine a connection point identifier, to determine a physical location based on the connection point identifier, including accessing a stored association between the connection point identifier and the physical location. The system can include the following features. The system can further include a location client in communication with the location module. The location client can communicate with the location module using a layer 2 protocol. The location client can communicate with the location module using a layer 3 protocol.

In another aspect, there is a method including determining, by one or more trusted network devices within a data network infrastructure, a physical location of a client device requesting access to the data network infrastructure to generate a trusted physical location and associating the trusted physical location with the client device.

The method can include determining whether a candidate network device is a trusted network device based on a probability that the candidate network device can be modified to provide false physical location data. The method can also include the following features. The method can further include prohibiting access to the one or more trusted network devices by anyone except authorized personnel.

One or more trusted network devices can be associated with a level of trust not less than a predefined threshold. The predefined threshold can vary based on a type of request by the client device. The trusted physical location can be associated with a level of trust. The method can further include determining the level of trust of the trusted physical location based on the one or

more network devices. The method can further include determining the level of trust based on a method of communication between the one or more network devices and the client device. The method can further include policing network activities of the client based on the trusted physical location.

The method also can further include determining a response for an access request by the client based on the trusted physical location. The method can further include controlling network resources provided to the client based on the trusted physical location. The method can further include transmitting the trusted physical location to an emergency response authority. The method can further include providing information to the client based on the trusted physical location. The method can further include providing information including points of interest within a predefined radius of the physical location.

In another aspect, there is a method that includes transmitting first location information from a trusted source within a data network infrastructure. The method also includes receiving second location information from a client device requesting access to the network, the second location information based on the first location information and determining a trusted location based on the first and second location information. In other examples, the method can include the following features. The method can further include policing network activities of the client based on the trusted physical location. The method can further include controlling network resources provided to the client based on the trusted physical location.

In another aspect, there is a method including determining a value for a physical location of a device. The method also includes determining a level of trust corresponding to the determined value and associating the level of trust with the value of the physical location. In other examples, the method can include the following features. The method can further include determining a level of trust based on a precision of a technique used for determining the value of the physical location. The method can further include determining a level of trust based on a granularity of a range of possible values used for determining the value of the physical location. The method can further include determining a level of trust based on a probability that determining a value can produce a false value for the physical location. The method can further include determining a level of trust based on a level of trust of a network device determining the value of the physical location.

In another aspect,, there is a system comprising a trusted network device within a data network infrastructure, the network device including a location module configured to determine a trusted physical location of a client device requesting access to the network infrastructure and to associate the trusted physical location with the client device.

In one aspect there is a method of determining a physical location of a device connected to a data network infrastructure including a plurality of connection points at different physical locations. The method includes receiving an operational signal characteristic from a device communicating with the data network infrastructure through one of the connection points and determining a physical location of the device, including accessing stored associations of signal characteristics with connection points. In other examples, the method can include the following features. The method can further include identifying the connection points with respective connection point identifiers. The device can connect to the connection point via a cable-based transmission medium.

The method also can further include measuring signal characteristics at each of the plurality of connection points and storing an association of a signal characteristic and its respective connection point for each connection point in the plurality. The method can further include employing a function that relates values for signal characteristics to respective physical locations. The signal characteristics can include a time delay. The signal characteristics can include time delay, time-domain reflectometry, signal attenuations, and/or round-trip delay.

In another aspect, there is a method for surveying a data network infrastructure including a plurality of connection points. The method includes determining a signal characteristic for a first connection point and providing to the network infrastructure the signal characteristic for the first connection point. The method also includes determining a signal characteristic for a second connection point and providing to the network infrastructure the signal characteristic for the second connection point.

In other examples, the method can include the following features. The method can further include storing a first association between the first connection point and its signal characteristic and storing a second association between the second connection point and its signal characteristic. The method can further include identifying the first and second connection points with respective first and second connection point identifiers. The method can further include connecting a location sensing device to the first connection point. The location sensing

device can comprise a GPS. The method can further include storing a third association between the first connection point and its physical location.

In another aspect there is a system including a transceiver and a location module. The transceiver is configured to receive an operational signal characteristic from a device communicating with a data network infrastructure through one of a plurality of connection points. The location module is configured to determine a physical location of the device by comparing the operational signal characteristic with a stored signal characteristic associated with the one connection point. In other examples, the system can include the following features. The location module can be further configured to employ a function that relates values for the signal characteristics to respective physical locations of the connection points. The location module can further include a signal characteristic database having an association of a signal characteristic and its corresponding physical location for each of the connection points.

In another aspect data is provided that includes location-based access control information. Access to the data at a physical location is then limited according to the location-based access control information.

This aspect can include one or more of the following features:

A physical location of a device accessing the data can be determined, and the limiting of the access is then according to the determined physical location.

Providing the data includes providing the data in encrypted form, and limiting access to the data includes enabling decryption of the data according to the physical location.

This aspect can have advantages, such as allowing data to be distributed to various locations, but only accessed at authorized locations. In this way, the actual location where the access is to be made can be used as part of the credentials, for example along with a password, that allow the data to be accessed. For example, if a file is loaded onto a disk on a laptop computer, the location of the laptop computer can determine whether the file can be opened. When the data takes the form of a computer file, the access limitations can then be hosted, for example, in operating system services or application programs that access the data.

In another aspect, there is a method including generating data including restrictive routing information based on physical location. In other examples, the method can include the following features. The method can further include transmitting the data in accordance with the restrictive routing information. The method can further include destroying the data if a network

device receiving the data is located at a restricted physical location in accordance with the restricted routing information.

The method can include prohibiting the data from being transmitted to a network device located at a restricted physical location in accordance with the restricted routing information.

The method also can further include prohibiting the data from being accessed by a client device located at a restricted physical location in accordance with the restricted routing information. The restricted routing information can include a prohibited physical location. The restricted routing information can include a permitted physical location. The data can include a data packet, a file, and/or a document.

In another aspect, there is a method including generating data for transmission via a network, the data including a physical location tag.

In yet another aspect, there is a method including receiving data at a first network device and prohibiting transmission of the data to a second network device based on a geographic physical location of the second network device.

In another aspect there is a method including receiving data at a device and prohibiting access to that data based on a physical location of the device.

In yet another aspect, there is a system including network devices and data. The network devices have associated physical locations. The data includes restrictive routing information based on a physical location. In other examples, the system can include the following features. The system can further include a physical location server having a storage module configured to store the associations of network devices with their respective physical locations. Each network device can include a storage module configured to store the association of that particular network device with its respective physical location. Each network device can include a location module configured to transmit the data in accordance with the restrictive routing information. Each network device can include a location module configured to destroy the data if the respective network device receiving the data is located at a restricted physical location in accordance with the restricted routing information.

Each network device also can include a location module configured to prohibit the data from being transmitted to another network device located at a restricted physical location in accordance with the restricted routing information. Each network device can include a location module configured to prohibit the data from being accessed by a client device located at a

restricted physical location in accordance with the restricted routing information. The restricted routing information can include a prohibited physical location. The restricted routing information can include a permitted physical location. The data can include a data packet, a file, and/or a document.

In another aspect, there are data including restrictive routing information based on physical location. The data can further include a header that includes the restricted routing information. This information may be represented explicitly, or using a tag to identify the information, for example, according to a registry of location information. The restricted routing information can be included in the network layer and/or in the transport layer. The restricted routing information can include prohibited physical locations. The restricted routing information can include permitted physical locations. The data can include a data packet, a file, and/or a document.

In another aspect, there is a method including receiving, at a first device, connection information from a neighboring network device and determining a physical location of the first device based on the connection information.

The method can include receiving, at the first device, the physical location transmitted from the neighboring network device. The physical location can be a first physical location and the neighboring network device can be a first neighboring network device. In this example, the method can further include receiving, at the first device, a second physical location transmitted from a second neighboring network device and comparing the first physical location with the second physical location to determine a level of confidence of an actual physical location of the first device. The method can further include associating a level of trust with the physical location based on the neighboring network device. The first device can include a router, a switch, a network entry device, a firewall device, or a gateway.

In another aspect, there is a system including a location module. The location module is configured to determine a physical location of a connection point and to transmit the physical location to a client device in communication with the connection point. The system can further include the client device, configured to receive the physical location from the physical location module, and a neighboring network device in communication with the client device, the neighboring network device including the physical location module. The physical location can be a first physical location and the neighboring network device can be a first neighboring

network device. In this example, the system can further include a second neighboring network device with a physical location module configured to determine a second physical location of the client device and transmit the second physical location to the client device. Further, the client device is further configured to receive the second physical location and to compare the first physical location with the second physical location to determine a level of confidence of an actual physical location of the client device. The system can associate a level of trust, based on the neighboring network device, with the physical location. The client device can include a router, a switch, a network entry device, a firewall device, a gateway, a wireless access point, and/or a computing device.

In another aspect, there is a method including receiving, at a network entry device of a network infrastructure, a request for network access from a client device. The method also includes determining, by the network infrastructure, a physical location of the client device and determining authorization of the client device based on the physical location. In other examples, the method can include the following features. The method can further include determining authorization by the network entry device.

The method can further include providing the physical location along with other user credentials to the authorizing device. The method can further include determining a level of service based on the physical location. The method can further include receiving, at the network entry device, user credentials, where determining authorization also includes determining a level of service based on the physical location and the user credentials. The method can further include authorizing a user associated with the client device if a level of trust associated with the physical location is not less than a predefined threshold. The method can further include communicating in accord with IEEE 802.1x.

In another aspect, there is a system with a network infrastructure. The network infrastructure is configured to determine a physical location of a client device. The network infrastructure includes a network entry device configured to receive a request for network access from a client device and determine authorization of the client device based on the physical location. The system can also include the following features. The network entry device can be further configured to determine a level of service based on the physical location. The network entry device can be further configured to receive user credentials and to determine a level of service based on the physical location and the user credentials. The network entry device can be

further configured to authorize a user associated with the client device if a level of trust associated with the physical location is not less than a predefined threshold. The network entry device can be further configured to communicate in accord with IEEE 802.1X.

In another aspect, there is an article for manufacture comprising a machine-readable medium that stores executable instruction signals that cause a machine to perform any combination of the methods described above.

The details of one or more examples related to the invention are set forth in the accompanying drawings and the description below. Other features, objects, and advantages of the invention will be apparent from the description and drawings, and from the claims.

DESCRIPTION OF DRAWINGS

FIG. 1 is a block diagram of an example system with location information;

FIG. 2 is a block diagram of an illustrative process employing location information;

FIG. 3 is a block diagram of another illustrative process employing location information;

FIG. 4 is a block diagram of another illustrative process employing location information;

FIG. 5 is a block diagram of another illustrative process employing location information;

FIG. 6 is a block diagram of another illustrative process employing location information;

FIG. 7 is a block diagram of another illustrative process employing location information; and

FIG. 8 is a block diagram of another example system with location information.

Like reference symbols in the various drawings indicate like elements.

DETAILED DESCRIPTION

1.0 Overview (FIG. 1)

Referring to FIG. 1, a location-aware system 100 operates and provides network-based services to users according to locations of devices that use or are part of the network associated with system 100. System 100 includes an infrastructure 101 that includes multiple switching devices, some of which are connected to connection points (e.g., 160a-i) of infrastructure 101. System 100 employs both hardware and software (e.g., an application executing on server 134) to provide location-aware services described below. A location of a device can relate to the

physical location of the device, which can be characterized in a variety of ways including as grid or map coordinates (e.g., latitude, longitude, and elevation), a geographic region, or in terms of building structures, such as coordinates on a particular floor in a building or a room number in a building. A device can be external to infrastructure 101 of system 100, such as user devices 104a and 104b. A device also can be internal to infrastructure 101, such as network entry devices 114a-b (sometimes referred to as switches or edge devices of the network), and a central switching device 136 (e.g. a router). The network entry devices 114 can include and/or be associated with wireless access points 120a-b. The wireless access points 120 can be individual devices external to the network entry device 114, such as 120a and/or internal to the entry device 114, such as 120b.

Some of the devices internal and external to infrastructure 101 include a location module 185. The location module 185 includes functionality, as described in more detail below, that makes a device location-aware. In one example, this functionality includes a location database to store location information, protocol to communicate location information to other devices, and rules to enforce location-based policies (e.g., to enable policing based on location information). This functionality can also include the algorithms and processes necessary to determine the location of a device using the techniques described herein. Location module 185 can be implemented in the hardware and/or software of system 100. For example, particular software applications executing on the devices can provide/enforce the location functions, the operating system of any of the devices can provide/enforce the location functions, and/or hardware modules, such as programmable arrays, can be used in the devices to provide/enforce the location functions.

To make use of a device's location, system 100 first determines the location of that device. System 100 uses different techniques to determine the location of a device depending on whether the device communicates with other devices using a cable-based transmission medium 112, or a wireless transmission medium 119. Cable-based transmission medium 112 refers to a constrained transmission medium such as an optical cable, an electrical wire, and the like. Such a cable transmission medium can provide single to many connections (shared) and/or a point-to-point (dedicated) connection between two devices. A cable-based medium 112 can be considered as part of infrastructure 101 of system 100. Typically the medium 112 is installed in such a way that it is not easy to modify the medium's physical location. For instance, cables are

lead through walls and conduits in such a way that the connection points (e.g., the jacks) are in fixed locations. Wireless transmission medium 119 refers to a transmission medium in a free space, such as though free air. Wireless transmission medium 119 generally relates to any communication where the transmission medium is air, for example, radio-based communication. For instance, radio communication according to the IEEE 802.11 standard uses a wireless transmission medium 119. Other wireless communication using wireless transmission media relate to use of optical communication (e.g., infra red, lasers, and the like) and/or other communications through air such as acoustic and mechanical waves. Wireless media are characterized by a much greater range of possible locations in which communicating devices may be located. For example, in the case of an IEEE 802.11 based network, a mobile device may be able to communicate with a wireless access point 120 hundreds or even thousands of feet away depending on the environment.

In the illustrated system 100 of FIG. 1, user device 104a connects to infrastructure 101 using cable 112 through connection point 160a (e.g., a jack in a wall). Similarly, network entry devices 114a-b and central switching device 136 connect to each other using a cable to connection points 160b-g. In a portion of a data network employing cables, a connection point (e.g., 160a-g) is the terminus of the cable where a device physically attaches. A connection port (e.g., 113) is the physical port through which a network client communicates.

As described above, the connection points associated with a cable are generally fixed in location. The locations of these connection points are determined, for example, when the cable is installed. Location information includes an association of a connection point with its corresponding location. System 100 stores the location information in location module 185. The location module 185 can store the location information using a location database. In an example of a centralized approach, system 100 stores the location information for all of the connection points of the network of system 100 in location module 185a in location server 134. In an example of a distributed approach, described in more detail in the alternatives section below, system 100 stores the location information for all of the connection points, or a portion of the connection points, in each of the location modules 185a-d. In one approach to determining the location of a device, system 100 determines the connection point (e.g., 160a-g) through which the device is connected to network infrastructure 101 and finds the stored location information in location module 185 corresponding to that particular connection point.

A device using wireless transmission medium 119 connects to infrastructure 101 through connection points 160h-i, for example communicating from the device's transceiver to the wireless access points 120a-b of network entry devices 114a-b, respectively. These wireless connection points 160h-i, similar to connection points 160a-g, are also generally fixed in location. The location of a user device 104 connected to a wireless connection point 160h-i, however, can be dynamic. The location of user device 104b changes as user device 104b moves. Stationary wireless connection points 160h-i may no longer be in communication with user device 104b as user device 104b moves away, thus no longer being connection points for 104b after a certain period of time.

In one approach to determining a location of a device using wireless transmission medium 119, system 100 determines the location of user device 104b relative to typically multiple network devices (e.g., 120a and 120b) that receive transmitted signals from user device 104b. System 100 uses signal characteristics, such as relative time delay or signal strength of the signal received at the different network devices in combination with the known location of the wireless access points 120a-b. System 100 optionally uses other known boundaries, for example walls within a building, to further limit the location of an area, relative to the wireless connection point (e.g., 120a or 120b), within which that user device 104 is operating. System 100 stores the location information corresponding to wireless user device 104b in association with one or more of the connection points 160h-i in location module 185 (e.g., 185a in an example of a centralized approach). The system 100 updates the corresponding location information as user device 104b moves.

Having determined the location of a device, system 100 employs that location information in a variety of ways. System 100 can provision and configure devices within infrastructure 101 or external to infrastructure 101 according to their locations as devices are added or moved. This enables a network device, in an automated fashion, to learn of its location and based on its location, configure itself, operate in a certain manner and enforce certain location-based rules. For example, network entry device 114a can be replaced with a new network entry device that, once connected, learns its location, and its configuration and rules of operation based on that location, in an automated fashion from location server 134.

System 100 is able to enforce certain restrictions, on an initial and continual basis, based on locations of devices. System 100 can restrict access to the network or data stored on the

network based on the location of user device 104. For example, system 100 restricts access to accounting databases to only user devices 104 located within the accounting department offices (e.g., within certain coordinates of a certain floor of a certain building). Further, system 100 can also periodically and/or continually police these restrictions so that a user device 104 cannot authenticate based on being in one location, and then try to access restricted services at another unauthorized location based on that authentication. Location can also be another parameter, for instance in addition to a user identification or a device type, that is used for allocation of network resources, such as speed and quality of service (QoS).

System 100 also restricts flow of data through infrastructure 101 based on location restrictions of that data. For example, the system 100 can restrict data from the accounting databases to stay within the accounting department offices (e.g., an area defined by certain coordinates). In one approach to implement such restrictions, the data has a tag that contains the location restrictions (e.g., permitted and/or prohibited locations). For example, the application generating the data and/or the server generating a data packet to transport the data over the network can add this tag while generating the data and/or packet. Devices and applications within system 100 enforce those restrictions by not allowing the data to be routed to a device outside of the permitted location, by destroying the data if it is in a location outside of the permitted location, and/or denying access to (e.g., reading, opening) the data outside a permitted location.

System 100 is also able to provide other services and applications that employ the location information. For example, system 100 can use the location information in emergency situations, where a device may be an alarm or sensor. System 100 determines the location of the alarm device and transmits the location information to a party responding to the alarm. System 100 can also use location information to recover a stolen user device 104. As the stolen user device 104 accesses the network, system 100 determines the location of the stolen device and transmits the location information to a party seeking to locate the device. System 100 can track mobile user devices (e.g., 104b) and thus can also track anything associated with that user device (e.g., the user, a file, a physical object, and the like). System 100, through the use of location information, can provide these and other services and applications. The sections below provide more detailed examples of the devices and techniques described in the above overview.

2.0 Locating Devices Overview (FIGS. 1, 2, and 3)

In determining the location of a device, system 100 employs one or more of a number of mechanisms/techniques so that location information can be verified and trusted by system 100. One general characteristic of these mechanisms is that devices or applications within infrastructure 101 do not necessarily trust devices outside infrastructure 101, even if those outside devices declare that they are at certain locations. That is, the determination of the location of a device is preferably based on information that is obtained directly by system 100 using network infrastructure 101, rather than supplied by a device itself. System 100 uses various approaches to obtain information to use when determining the location of a device communicating with the network, with some specific approaches being applicable to cable-based or wireless transmission media.

In general overview, for wireless devices (e.g., devices communicating via a wireless transmission medium), system 100 maintains information that is used to locate the devices based on the characteristics of wireless communication between typically multiple devices (e.g., 120a and 120b) in network infrastructure 101 and a wireless user device (e.g., 104b). Generally this approach is referred to as triangulation, with the understanding that this includes all varieties of remote location determination and approximation including those based on variations in time delay, signal strength, and directionality of signals based on the location of a wireless device, and including both analytical or model-based approaches as well as approaches that are based on prior measurement and recording of transmission and propagation characteristics at various locations.

For devices connected via cable, system 100 maintains information that characterizes the locations of the cable connection points, for example in a location database stored in location module 185. Such a database is populated and maintained in a variety of ways. For example, once network infrastructure 101 has been physically arranged, a survey of all the cable connection points can be undertaken to record the physical location corresponding to each cable connection point 160 and its corresponding connection port in network infrastructure 101. Then, as a device or the network infrastructure identifies a cable connection point 160 to which the device is connected, system 100 uses the location database to determine the location corresponding to the identified connection point. The connection points are identified using a

unique connection point ID. The value of the connection point ID can be, for example, a number, a text string, or a combination of infrastructure pertinent information.

After determining the location of a device using one of these techniques, in one example system 100 maintains the location information centrally on the location server 134 in the location database in location module 185a. In the case of wireless devices, system 100 dynamically modifies the location of the device stored in the location database as the device moves. System 100 can track the user device itself, and/or the closest network entry device (e.g., 114) through which the wireless user device communicates. With the devices that communicate via a cable, system 100 updates the location database if and when a device is moved from one cable connection point (e.g., wall jack) to another. The devices communicate the location information to each other using a protocol using layer 2 (the data-link layer) or layer 3 (the network layer) of the Open Systems Interconnection (OSI) communication model. For example, the devices communicate with each other using IP version 4. Other layers and protocols can also be used. Additional and alternative mechanisms for locating devices are described further below in the alternatives section.

2.1 Techniques for Determining Location of Connection Points (FIG. 1)

Following below are examples of more detailed mechanisms/techniques to determine the location of the connection points, thus determining the location of the devices employing those connection points. The detailed descriptions of various mechanisms are divided into those mechanisms most applicable to wireless connections (i.e., connections using a wireless transmission medium) and those mechanisms most applicable to cable connections (i.e., connections using a cable-based transmission medium), although in general, mechanisms may be applicable to both types of connections. There can be examples when the mechanisms can be applicable to other types of connections (e.g., mechanisms for cable connections can be applicable for wireless connections).

2.1.1 Wireless Connections (FIG. 1)

Referring now to some detailed techniques for wireless connections, as described above, two example types of wireless communication chosen to illustrate these techniques are via radio frequencies or infrared frequencies. System 100 can employ different mechanisms for each of these types of communication. System 100 can employ a first group of mechanisms/techniques for identifying the location of a device (e.g., 104, 114) that communicates via radio frequencies. For example, system 100 triangulates the location of a device using one or more wireless access points, such as 120a-b, associated with network entry devices 114, such as 114a and 114b, respectively, as shown in Fig. 1. As another example, system 100 determines a device's location based on the proximity to an entry device. Following below is a listing of various techniques system 100 can employ to determine the location of a wireless device.

System 100 can employ a number of known triangulation techniques, including the use of signal strength, angle of arrival, and relative time delay approaches. System 100 can employ off-frequency searching, such as by frequency hopping for short periods of time to detect stations on frequencies alternate to that employed for data exchange. For example, wireless access point 120a can operate at a first frequency f1. Wireless access point 120b can operate at a second frequency f2. Periodically, and for a relatively short period of time, wireless access point 120a operates at the second frequency f2 to detect and determine signal characteristics of a device communicating with wireless access point 120b. Similarly, wireless access point 120b periodically and for a relatively short period of time operates at the first frequency f1 to detect and determine signal characteristics of a device communicating with wireless access point 120a.

System 100 can employ phased-array searches for lobe-based triangulation. That is, a radio antenna of the network entry device is directed to maximize or at least optimize lobe location as a search beacon. Such lobeing or lobe steering may be a staged process in which network entry devices 114 make broad sweeps to get rough location information, which may be sufficient in some situations. Network entry devices 114 can fine-tune the sweeps, if desired, with narrower lobes, to get a more accurate location. System 100 also can conduct phased-array antenna searches at off-frequency conditions (e.g., frequency hopping combined with directional searching).

System 100 can perform calculations to approximate distance from a known access point (e.g., 120a-b) as a function of signal strength attenuation (e.g., the signal is at x strength so the device must be located in a range of y-z feet away). In addition to calculations, system 100 can also search stored associations of signal characteristics and their corresponding locations. This information can be stored in a signal characteristic database. A network administrator generates this signal characteristic database by measuring predefined signal characteristics at different locations and storing the measured characteristics for each of the locations. When subsequently determining a location of a user device, if system 100 detects a signal characteristic identically corresponding to a location, system 100 determines that the user device is at that corresponding location. If the signal characteristic is not identical, system 100 can use multiple entries within the database to extrapolate the user device location information based on the stored signal characteristic and location associations. This technique is sometimes referred to as RF training.

Using multiple frequencies and/or connection-points and/or antennas may improve the accuracy of location derivation techniques. For example, if the same access point is used at different frequencies, system 100 can use the error in location information among the different frequencies to infer location more accurately. In addition, the use of multiple access points (e.g., signals from user device 104b received at 120a compared with signals received at 120b) may improve relative location accuracy in a type of triangulation or averaging of signal strength indicators. System 100 can employ multiple antennas for that purpose. Multiple antennas (not shown) may also be used to assert a line of bearing. In that case, the relative separation of the antennas and the accuracy of the known spacing both may provide improved location accuracy. System 100 also can employ ultra wide band waves to determine relative location of one or more devices. As the accuracy of the location derivation increases by using these improved techniques, system 100 can assign a higher value for the level of trust parameter associated with that location.

System 100 also can use signal amplitude differential from the network entry devices 114a and 114b to determine relative location of user device 104b with respect to an antenna on network device 114a or 114b. System 100 can combine techniques, such as using signal amplitude differential combined with the phase differential techniques described above to determine location. The location techniques described are not limited to any specific type of antenna technology. System 100 can employ an antenna associated with a wireless access point

120, or an antenna associated with a stand-alone device, including, but not limited to, a personal digital assistant or a laptop computer, designed to relay information to a network-related device employed to calculate relative location from received data. One or more antennas can be deployed in one or more wireless access points 120. System 100 can also vary and limit the transmission strength of the wireless access points 120, so that system 100 can determine and control a radius of relative location based on the radius of operation due to the limited transmission strength. This relative location can be further limited from the radius of operation by other physical barriers such as walls and non-accessible locations within the radius of operation.

System 100 also can employ a second group of mechanisms for identifying the location of a wireless device (e.g., 104, 114) that communicates via optical technology, such as infrared light waves and lasers. More specifically, the use of an infrared transmitter and receiver can limit the actual distance user device 104b can be from a network entry device 114a or 114b, similar to the limited transmission strength above. Thus, system 100 determines a relative position of user device 104b using that maximum distance limit as a radial boundary from network entry device 114a or 114b. Further, a line-of-site requirement for infrared can limit the boundaries further, although reflective devices can be used to alter such limitations. As described above, system 100 can use physical barriers, such as walls, to limit the determined boundaries of the allowable locations of the infrared device.

System 100 uses the techniques above for radio and infrared communications to determine the location of a wireless device. As described in more detail below, system 100 may use the above techniques to determine the absolute location of wireless user device 104b itself, or use the above techniques to determine a relative location, determining whether wireless user device 104b is closer to wireless access point 120a or 120b and using other known parameters, such as transmitter strength and physical barriers. The location information gathered by system 100 (e.g., via access points 120a and 120b) using the above techniques may be considered trusted information if the network-controlled devices (e.g., access points 120a and 120b) collecting the information are trustworthy. The devices are considered trustworthy if, for example, they are part of infrastructure 101 and cannot be accessed, moved, and/or modified by anyone except authorized network administrators. Instead of receiving a location from a wireless device and relying on that received information as accurate, system 100 verifies the location of a device

itself using one or more of the above techniques. Determining location information for an authenticated user by trustworthy devices (e.g., a device within infrastructure 101 that cannot be altered) enables system 100 to assign to the location information a higher value for the level of trust and enables greater security in the permitted access to system 100 as described in more detail below.

2.1.2 Cable Connections (FIG. 1)

Referring now to some detailed techniques/mechanisms to determine a location of a device using cable connections, system 100 can search locations of connection points previously stored in a location database and/or system 100 can use characteristics of signal propagation through a cable-based transmission medium. In one example, system 100 searches a location database to find the location of a connection point to which a device is connected. The database is located in location module 185 of location server 134. As described below, system 100 assigns a unique identifier to each connection point 160. When a device connects to system 100, system 100 determines the unique identifier of the cable connection point to which that device is connected. System 100 searches the location database to find the connection point with that unique identifier and uses the location that corresponds to that connection point. To use this technique, the location database is populated when the cable connection points are installed and/or when the connection points are first used.

The process to generate the database can be manual and/or automated. In an example of a manual process, a network administrator enters the unique identifier for each connection point and its corresponding location in the location database. For example, the network administrator uses a map (e.g., floor plan, office layout, and the like) to determine the location information of each of the installed connection points. The location information obtained from the map and entered into the location database can include coordinates of the connection point (e.g., lat 42°, long 48°), a string description of the connection point (e.g., room ten, first floor, building one) and the like.

In an example of an automated process, system 100 uses user device 104 with its own location determining system (e.g., GPS) to provide system 100 with location information as user device 104 is connected at each connection point 160. The system 100 can employ a trusted user

device (e.g., a user device with no/low probability of providing false location information or always under control of a network administrator) or an untrusted user device (e.g., a device not under the control of the network administrator).

With an untrusted user device, system 100 can attempt to independently verify the location information received from the untrusted device. For example, if the untrusted device can use both cable-based and wireless transmission media (e.g., a laptop with a network card and a wireless transmitter or infrared port), system 100 can use one or more of the wireless techniques above to verify the location of the device while the device communicates using a cable connection point. System 100 can also use one or more of the signal characteristic techniques below to verify the location of the device while the device communicates using a cable connection point.

With a trusted user device with its own location determining system, as system 100 determines the connection point to which the trusted user device is connected and receives the location determined by that trusted user device, the system 100 adds an association of the connection point and its corresponding location to the location database. When the trusted user device connects to additional connection points, system 100 populates the location database further until all connection points have corresponding locations. In the association, system 100 can use a unique identifier to identify each of the connection points.

In another example of an automated process, system 100 employs a trusted user device 104 with its own location determining system that can work in the absence of GPS data. System 100 employs a user device with standards-based LAN connectivity capabilities. The user device is capable of determining an absolute 3-dimensional position via GPS and also has the capability, likely via an inertial navigation system, to determine its absolute position in the absence of GPS data. An inertial navigation system may be preferred because the GPS uses very low power transmissions from the satellites and reception indoors or even outdoors in heavily developed areas may be poor or non-existent. If system 100 provides a start or reference position to an inertial-based system, that system can maintain very accurate 3-dimensional location datum with no external information. In addition to the starting position, system 100 can provide a security feature to the user device to ensure that its location information is trustworthy. This can include, for example, keys and laser techniques. The user device calculates absolute position information, and has the capability to format that information for IP transport over a LAN via its

LAN interface. An operator can go to a port providing access to the LAN, connect the trusted user device to that port, and command that the current location information derived by the user device be sent to the location database in the location server 134. Upon receipt of that information, system 100 updates the location information in its location database for that connection point.

In another example, as described in more detail in the alternatives section, a trusted third party can act as an agent to provide the location of connection point 160a. For example, if the connection point 160 is a telephone jack in a user's home, the corresponding telephone number can be used as a connection point ID. The telephone company can act as a trusted agent and provide a location (e.g., residential address) of that connection point. System 100 assigns a value for the level of trust parameter associated with that location information based on the trustworthiness of the source, as described below. The more system 100 trusts the third party agent, for example the phone company, the higher level of trust system 100 associates with the provided location information.

As an alternative or in addition to the predefined database, system 100 can use characteristics of signal propagation through a cable-based transmission medium to determine the location of a device. More specifically, system 100 can use a characteristic of a signal that varies with the length of the cable-based transmission medium (e.g., time delay, time-domain reflectometry (TDR) techniques, signal attenuations, round-trip delay and the like) to determine the length of cable through which the signal is traveling. For a connection point, system 100 measures the particular signal characteristic and based on that measurement, system 100 determines the length of the cable. As described above for wireless connections, system 100 employs a lookup table, database, and/or function that relates the characteristic measurement to a location for cable connections also. Data for the signal characteristics (e.g., round-trip training for cable-based media) can be performed at the same time connection points 160 are being mapped with a trusted GPS, as described above, so that location is not based solely on estimating delay.

For example, a signal characteristic database contains the association that a measured time delay of a signal corresponds to a specific length of cable from the network entry device 114a. System 100 determines a relative position of user device 104a using that determined cable length as a maximum distance from connection point 160a by accounting for (e.g., subtracting)

the length of cable 112 included in the infrastructure. Further, as described above, system 100 can use physical barriers, such as cable runs and walls, to limit the determined boundaries of the allowable locations of the user device 104a. This technique is useful in determining whether user device 104a is connected to connection point 160a using a long length of cable, thus allowing user device 104a to be located a substantial distance away from the connection point 160a (e.g., in a different, and perhaps unauthorized, room). For example, system 100 determines, using signal characteristics as described above that there is 10 feet of cable between user device 104a and network entry device 114a. System 100 has information that the cable length from connection point 160a to 114a is 7 feet and is fixed (i.e., runs through a wall and cannot be modified). Using this combined information, system 100 determines that the length of cable from connection point 160a to user device 104a is 3 feet and so the user device 104a is confined to the room in which connection point 160a is located.

The use of signal characteristics also enables system 100 to determine which connection point a user device 104 is connected to for cables with multiple connection points (e.g., 104i and 104j, FIG. 8). For example, system 100 can use a calculated cable length to determine which of the connection points user device is within the range of the cable length. Once a connection point is identified, system 100 can obtain its location via the location database and then determine the location of the user device 104. It may be the case that system 100 identifies multiple connection points within the range of the cable length. It some instances, this may still be enough to authenticate the location, as described in more detail below. For example, the cable length may indicate that the user device is connected to one of the connection points in conference rooms 1-5 on the second floor. All of the conferences rooms, however, are in permitted locations for the requested network resources, so this granularity and precision is acceptable for authentication in this case.

2.2 Location Information Database (FIG. 1)

As described above for both wireless and cable-based transmission media, system 100 maintains and updates the location information associated with the connection points (e.g., 160a-i) of the system 100 in a location database. The information included in the location database can vary. For example, Table 1 is a table containing the type of information that can be included

in the location database. As illustrated in Table 1, each row represents an association between a connection point and its corresponding location in one or more formats. The "Connection Point ID" column contains the unique identifier associated with a particular connection point. The connection point ID can be any ID that uniquely identifies a connection point. As described in more detail below and illustrated in Table 1, in one example the combination of a device Media Access Control (MAC) address (e.g., 00001d000001) and a port MAC address within the device (e.g., 00001d000101) determines the connection point ID. The locations contained in Table 1 are included in two format types for each connection point ID. The first type is an American National Standards Institute (ANSI) Location Identification Number (LIN) and the second type is a coordinate of latitude and longitude. (Some additional example formats system 100 can employ are described in the alternatives section below.)

The location information of Table 1 additionally includes the optional parameters "Level of Trust" and "Device ID". The level of trust, as explained in more detail below, is a parameter with a value in a predefined range, where the range represents the trustworthiness of the location reference. The level of trust generally corresponds with the trustworthiness of the source providing the location of the connection point. A higher level of trust value represents a higher level of confidence that the location reference is accurate, reliable and has neither been altered or generated falsely to gain normally unauthorized access. The device ID uniquely identifies the device that is connected to the connection point. The device ID information enables system 100 to store a map of the physical locations of all the network devices (e.g., 104, 114, 136). This is beneficial if there are devices associated with system 100 that are not configured to acquire and/or store their location information. System 100 can use this corresponding device information to enable location server 134 to transmit location information to a location-aware application since the device cannot transmit the location information itself. IN other words, system 100 can act as a third-party verifier for applications requiring verified location information. Table 1 can include other information in addition or as an alternative to the device ID. For example, Table 1 can include MAC address, address, phone number, protocol type, asset ID, owner and/or the like.

Connection Point ID	Location ID Type	Location Reference	Location ID Type	Location Ref.	Level of Trust	Device ID
00001d000001: 00001d000101	ANSI LIN	xxxxxxxxxx1	Lat-Long	x1° by y1°	2,256	Model: ABC S/N: 123
00001d000001: 00001d000102	ANSI LIN	xxxxxxxxxx2	Lat-Long	x2° by y2°	2,256	GUID: A82C3
00001d000001: 00001d000103	ANSI LIN	xxxxxxxxxx3	Lat-Long	x3° by y3°	2,256	
00001d000001: 00001d000104	ANSI LIN	xxxxxxxxxx4	Lat-Long	x4° by y4°	2,256	
00001d000001: 00001d000105	ANSI LIN	xxxxxxxxxx5	Lat-Long	x5° by y5°	2,256	
00001d000001: 00001d000106	ANSI LIN	xxxxxxxxxx6	Lat-Long	x6° by y6°	2,256	
00001d000001: 00001d000107	ANSI LIN	xxxxxxxxxx7	Lat-Long	x7° by y7°	2,256	
00001d000001: 00001d000108	ANSI LIN	xxxxxxxxxx8	Lat-Long	x8° by y8°	2,256	
00001d000001: 00001d000109	ANSI LIN	xxxxxxxxxx9	Lat-Long	x9° by y9°	2,256	
00001d000001: 00001d000110	ANSI LIN	xxxxxxxxx10	Lat-Long	x10° by y10°	2,256	

Table 1

2.3 Specific Examples of Locating Devices (FIGS. 1, 2, 3, and 8)

As described above, once the location database is established, system 100 can provide the location information to a device when that device connects to a connection point. This can include providing location information to devices outside of infrastructure 101 as well as devices within infrastructure 101. FIGS. 2 and 3 illustrate additional examples of system 100 locating devices. FIG. 2 broadly illustrates the steps system 100 performs, from discovering a device's connection to system 100 to allowing the device access to the network. FIG. 3 illustrates more specifically the steps system 100 performs to determine the location of the discovered device. In other words, FIG. 3 shows a portion of the steps of FIG. 2 in more detail.

FIG. 2 broadly illustrates an example of a sequence of steps system 100 performs, from discovering a device's connection to system 100 to allowing the device access to the network.

Referring to the example location identification process 201 of FIG. 2, system 100 activates or otherwise discovers (step 210) a device destined for a network association, or a device already network associated. System 100 queries (step 215) the device for location information. That location information may be of absolute or relative type. If location information does not exist, system 100 queries (step 220) whether the device can identify its own location. If the location information does exist, or the device can provide a trustworthy location, system 100 establishes (step 230) the device location information. A location is trustworthy, for example, if the system 100 assigns a level of trust value for that location that is above a predefined threshold. The predefined threshold can vary depending on the network resources that the device requests. For example, sensitive information and applications require a much higher threshold than access to public information.

If the device cannot provide its own location information, or the location information is not associated with a level of trust acceptable to system 100 for the particular transaction requested, the location information is determined (step 225) independently of the device, by system 100 itself or a trusted third party agent. After determining (step 225) a trustworthy location, system 100 establishes (step 230) the device location information.

Whether system 100 can trust the location information from a device (e.g., associate a high enough level of trust value with the location) can depend on the source of that location information. For example, if the location information came from a secure device within infrastructure 101 not vulnerable to modification, system 100 can trust the location information and assign a the location information a high level of trust value. If the location information came from a GPS and/or has been verified by a third party certificate with security features allowing for a low level of probability of providing a false location, system 100 can trust the location information, but with a lower level of trust value than if the location information came from system 100 itself. The range of level of trust values is described in more detail in the restricting access section below.

In one example where system 100 determines (step 225) the location of a device, thus assigning a high level of trust value to that location, the device receives connection information from a network entry device (e.g., 114a, 114b). The connection information includes information that the network entry device has, such as a network entry device identifier and a port number of the network entry device to which the connection point is connected. The device

transmits the received connection information, or a portion thereof, to system 100, or more specifically, to a portion of the network maintaining the location information database (e.g., location server 134). Using the received information (e.g., network entry device identifier and port number), location server 134 determines the connection point to which the device is connected. Referring to the unique identifier of that connection point, which in one example could be the combination of the network device identifier and port number, location server 134 retrieves the location associated with that connection point. Location server 134 transmits to the device the location information associated with the connection point.

Continuing with process 201, system 100 optionally confirms (step 235) a predefined list of additional parameters, either through a database search or a table update. System 100 may employ that predefined list of parameters to define network access as described below. The predefined list of parameters may include, but is not limited to, the device port number of the connection, traffic activity and link information, MAC address, IP address, a timestamp, and activity staleness. Upon satisfaction by system 100 that the appropriate predefined list of parameters and device location information has been gathered (step 235), system 100 permits (step 240) network access. As described below, the location information may be used as a supplement to existing network usage control means, such as NOS, RADIUS, IEEE 802.1X, IEEE 802.1Q, firewalls, and QoS mechanisms. Further, system 100 continually polices against these mechanisms to ensure that network usage does not go beyond the bounds set by parameters defined within these mechanisms, including location restrictions for devices and/or data.

In general, in alternative sequences of steps, system 100 establishes a device location and a level of trust of that established location based on a combination of multiple inputs, including location information included in the device itself (e.g., step 215), location information identified by the device (e.g., step 220), and location information gathered independently of the device (e.g., step 225), without necessarily following the sequence shown in Fig. 2.

In addition, Fig. 2 shows a single sequence of steps to determine a location of a device and to act on that determined location. In general, this process, and other processes involving determining or verifying device locations that are described below, may be repeated while the device is connected to the network for any of a number of reason of interest to the network admin that re-determining location is required, including in the event of a detected attack, when new information about the device's location becomes available, periodically, or based on an

internal or external network events or other matters of network policy. This repetition of the process provides an ongoing policing function. For example, such a policing function can be used so that a device cannot be established at one physical location, and then moved to another physical location where its privileges may be different.

As introduced above, a wide variety of events may initiate the process of determining and validating the location of a device. These can include, but are not limited to: a timer expiring, a communication link being broken, a communication session terminating, a change in a user's credential, triggering of a firewall alarm, a new network device joining the network, prompting by a management station, particular movement of a device is detected, a shadow (users or devices of network) device is detected.

Referring to FIG. 3, example process 300 illustrates the steps system 100 performs to determine the location of the discovered device. For clarity and example only, some portions of example process 300 refer to a location server and a location client. A location server refers to a device of system 100 comprising functionality in location module 185 that enables that device to provide location information to another network device. This can include hardware and/or software applications for the storage of location information parameters, access to the storage devices containing values for parameters, algorithms and processes to determine the location of a device and other like functionality. Additionally, location module 185 of a location server may be further configured to provision operational configuration parameters based on the location of the network-attached device, as illustrated in the optional steps of FIG. 3. A location client refers to the device for which the location server is trying to determine location. The network entity of FIG. 3 represents an intermediary device that includes the access port through which the location client communicates.

Referring to FIG. 1, for an example where the location client is user device 104a, the network entity of FIG. 3 is the network entry device 114a, which has connection port 113 through which the user device 104a communicates. For an example where the location client is network entry device 114a, the network entity of FIG. 3 is the switching device 136, which has the connection port 165 through which device 114a communicates. As these two examples illustrate, network entry device 114a can act as both a location client and an intermediary device. In a distributed example described in the alternatives section below, network entry device 114a also

can act as a location server, thus combining the network entity and the location server of FIG. 3 into a single device.

Referring to process 300, the network entity (e.g., 114a) transmits (step 305) connection information (e.g., in the form of data packets) to the location client (e.g., 104a) that allows for the detection of a unique connection point ID. This connection information can represent the port to which the connection point is physically connected. The connection information can be in a format compliant with many different protocols. The location client receives (step 310) the connection information and determines (step 315) a connection point ID. For example, the location client can extract the connection point ID from one of the example packet types.

For illustration, a specific example employs IEEE Spanning Tree Bridge Protocol Data Unit (BPDU). In an IEEE 802.1 D Spanning Tree BPDU example, every switch port with spanning tree enabled will forward (step305) a BPDU at regular intervals. A BPDU comprises the following information: (i) the primary MAC Address of the transmitting switch (bridge ID); (ii) the identifier of the transmitting port (the MAC address of the switch port sending the BPDU); (iii) the unique bridge ID of the switch that the transmitting switch believes to be the root switch; and (iv) the cost of the path to the root from the transmitting port. The location client receives (step 310) the IEEE spanning tree BPDU and decodes the unique bridge ID and transmitting port ID as its connection point ID. Using that decoded information, the location client determines (step 315) that the connection point ID={Bridge ID MAC Address}+{Transmitting Port ID MAC Address}. Alternatively, the location client forwards these received parameters to the location server and the location server generates the connection point ID by combining the applicable parameters, as described in FIG. 2.

It can be seen that this approach may be applied to other discovery protocols and techniques, with modification dependent upon specific protocol formatting. Also, system 100 can employ other unique identifiers. For example and referring to FIG. 8, for user device 104h, which is connected to system 100' through a telephone network 132, system 100' can employ a phone number to uniquely identify the connection point 160k (e.g., phone jack) to which the user device 104h is connected. Similarly, user device 104g can be a personal computer connected to Internet 148 via a cable modem that has been assigned a unique IP address. System 100' can employ this unique address, alone or in combination with an ISP identifier, to uniquely identify

the connection point 1601 (e.g., a jack or the end of a cable for a cable modem) associated with user device 104g.

In process 300, the location client transmits (step 320) the connection point ID to the location server. The location server determines (step 325) location information for the location client based on the connection point ID. The location information can be defined in a location database within the location server as described above or discovered from the network infrastructure 101' using the techniques described above.

After determining (step 325) the location information, the location server transmits (step 330) the location information to the location client. If configured to do so, the location client stores (step 335) the location information for future reference. In addition to the location, the received data may include a corresponding level of trust value associated with the origination of the location information. The location information, and any additional information, may also be protected with a security feature. For example, the information may be encrypted with a temporary key associated only with the particular connection point to which the location client is connected.

To determine (step 325) location information, the location server employs a location database comprising connection point ID information and geographic information. An advanced location server can also act as a device registry and can map unique identifiers of the devices (e.g., 104, 114) to their corresponding connection point and geographic information, as illustrated in Table 1 above. As illustrated in FIG. 3, the location server can optionally store (step 340) the location information in a storage module on the network entity. In another example, the network entity storage module and the location database can be the same. Thus, more than just a topology, the location server stores and/or has access to information with the physical locations of the mapped devices.

Referring to process 300, the location client counts (step 320) a predefined amount of time to resend (step 320) its connection point ID information to the location server periodically to ensure the accuracy of the location information. The location server sends (step 330) the location information to the location client after referencing (step 325) the connection point ID that was previously sent by the location client. This periodic verification is one example of system 100 periodically policing location information. Or in other words, periodically verifying that the location client has not changed locations.

Also shown in process 300 are the optional steps 350 and 355, representing examples where the location server is expanded to provision and/or store information other than the location references in the location database. In this example, the location server obtains (step 350) configuration and/or provisioning information based on the connection point ID and transmits this additional information to the location client. Using this additional information, the location client can configure (step 355) itself in accord with this additional data, which is based on location. Similarly, although not shown, the network entity can also configure itself.

After system 100 authenticates the location information and optionally configures devices based on their location, system 100 continually polices the network at the edges of infrastructure 101 to ensure that policies regarding location information are enforced. The steps 365, 370, 375, and 380 of process 300 illustrate an example of edge policing by system 100. For example, when the location client requests (step 365) additional resources, the network entity (e.g., in the case of edge policing, network entry device 114) verifies (step 370), using any of the techniques described herein, that the location client is still at the same location as when the client was authenticated. If not, the location client is forced to repeat the authentication process at the new location. In response to a request for data, the location server, or another server and/or application on the network, transmits (step 365) the requested data to the location client via the network entity. As described in more detail below, the network entity determines whether there are any location restrictions on the data. If so, the network entity enforces (step 380) those location restrictions by, for example, not forwarding the data to the location client if the location client is at a prohibited location. As illustrated, the network entity polices both incoming requests and outgoing data in accordance with location based policies.

3.0 Network Operation Using Device Location (FIGS. 4, 5, 6, and 7)

As illustrated in the optional steps of FIG. 3, once system 100 determines the location of a device, system 100 can employ that location information to provide some automated operations. In other words, a network that is location-aware enables the utilization of information stored on a location client and/or in the location database to enhance the operation of the location-aware network. Because system 100 is able to learn the connection point to which any device is connected using the techniques above, system 100 can provide automated management based on

the locations associated with those connection points. The operations and services that the system 100 provides for automated management based on location information vary. Some techniques/mechanisms are described below in more detail.

3.1 Provisioning and Configuring

One type of automated mechanisms involves the provisioning and configuration of devices as they are added to system 100. When added, system 100 determines the location of the added device and then based on that location, system 100 determines, for example, what particular configuration file should be loaded into the device, what type of network priorities the device should be assigned, such as bandwidth, latency, QoS and other like network policies. This mechanism enables system 100 to enforce any of these policies based on the location of each device. The examples that follow illustrate how system 100 can expand data within the location database to include the provisioning and/or configuration data.

3.1.1 Provisioning/Configuring Examples Using an Expanded Location Database

In one specific example of provisioning, a location server assigns location information and network specific configurations to Voice over IP (VoIP) handsets. The information is provisioned on the phone and includes, for example, Virtual LANs (VLANs) ID, traffic prioritization at layer 2 or layer 3, and an E911 LIN. This simplifies the information on VoIP phones in branch offices, for example. The provisioned parameters are added to the location information in the location database of the location server. An expanded location database for VoIP phone environments can include the following information: VLAN membership of the voice entity, layer 2 priority mappings for voice payload/voice control/non voice traffic, layer 3 class of service markings for voice payload/voice control/non voice traffic, location client's network layer address, ANSI LIN numbering, geographic location information including latitude, longitude, altitude and accuracy factor, device microcode file to boot (e.g., bootp server pointer), and/or other like parameters. Table 2 is a table containing an example of the type of information that can be included in an expanded location database that includes additional provisioning parameters for a VoIP network. In addition to the connection point ID and the location reference,

the location database represented by Table 2 also includes a voice VLAN ID and a voice priority parameter. As described above, the location database also can include device ID data about a location client. In the VoIP example, these optional device ID parameters can include the handset extension number, the handset model number, the handset version, the handset network address, and/or the like.

Entry	Connection Point ID	Location ID Type	Location Reference	Voice VLAN ID	Voice Priority	Device ID (optional)
1	00001d000001: 00001d000101	ANSI LIN	xxxxxxxxx1	101	5	extension: 7082 model: 123
2	00001d000001: 00001d000102	ANSI LIN	xxxxxxxxx2	101	5	
3	00001d000001: 00001d000103	ANSI LIN	xxxxxxxxx3	101	5	
4	00001d000001: 00001d000104	ANSI LIN	xxxxxxxxx4	101	5	
5	00001d000001: 00001d000105	ANSI LIN	xxxxxxxxx5	101	5	
6	00001d000001: 00001d000106	ANSI LIN	xxxxxxxxx6	101	5	
7	00001d000001: 00001d000107	ANSI LIN	xxxxxxxxx7	101	5	
8	00001d000001: 00001d000108	ANSI LIN	xxxxxxxxx8	101	5	
9	00001d000001: 00001d000109	ANSI LIN	xxxxxxxxx9	101	5	
10	00001d000001: 00001d000110	ANSI LIN	xxxxxxxxx10	101	5	

Table 2

In one specific example of configuring, a location server enables automated configuration of location clients, such as switches and routers. Often, network switches have to support complex configurations, and that complexity limits the ability of the switch to be moved around the network. If system 100 enables a network switch as a location client, it is possible to automate the configuration of the network switch. In this example, a network operator enters a wiring closet and simply plugs in a network switch that only contains its network layer address and the network layer address of the location server. After the network switch powers up, it detects (step 310 (FIG. 3)) its location, for example as described above, by analyzing an IEEE

Spanning Tree BPDU to determine (step 315 (FIG. 3)) its connection point ID. Once the network switch determines (step 315 (FIG. 3)) its connection point ID, the network switch initiates (step 320) a conversation with location server 134. In this example, the location server references (step 350 (FIG. 3)) the connection point ID to a location database field which represents the base configuration file of any network switch that may connect to the network at that location. Table 3 is a table containing an example of the type of information that can be included in an expanded location database that includes additional configuration parameters to configure a network switch. In addition to the connection point ID and the location reference, the location database represented by Table 3 also includes a configuration file parameter identifying the configuration file to be used to configure a location client at that corresponding location.

	Connection Point ID	Location ID Type	Location Ref.	Configuration file
1	00001d000001:00001d000101	Lat-Long	x1° by y1°	closet1.cfg
2	00001d000001:00001d000102	Lat-Long	x2° by y2°	closet2.cfg
3	00001d000001:00001d000103	Lat-Long	x3° by y3°	closet3.cfg
4	00001d000001:00001d000104	Lat-Long	x4° by y4°	closet4.cfg
5	00001d000001:00001d000105	Lat-Long	x5° by y5°	closet1.cfg
6	00001d000001:00001d000106	Lat-Long	x6° by y6°	tftp:/1.1.1.1/closet15.cfg
7	00001d000001:00001d000107	Lat-Long	x7° by y7°	closet1.cfg
8	00001d000001:00001d000108	Lat-Long	x8° by y8°	http:/2.2.1.1/closet99.cfg
9	00001d000001:00001d000109	Lat-Long	x9° by y9°	closet1.cfg
10	00001d000001:00001d000110	Lat-Long	x10° by y10°	ftp://3.3.3.3/config10.cfg

Table 3

3.2 Restrictions Based on Location (FIGS. 4, 5, and 6)

In addition to provisioning and configuring, the operations of system 100 can be restricted based on location. These restrictions can involve restrictions on the access and use of system 100. These restrictions also can involve the transmission of data around and through system 100. For an overview example relating to network access, the location information within a network enables authentication based on location. Location information allows system 100 to authenticate a user not only based on the credentials provided by the user, but also based on the location of the device used by the user to access the network. Dependent upon the device location, system 100 can allow or restrict access to certain devices, information, applications,

signal exchange priorities, and the like. Further, even if a device and/or its user supplies to system 100 a claimed device location, system 100 can employ the techniques described herein to confirm the location independently from the device. This ensures that the device location comes from a trusted source (e.g., assign an acceptable value for the level of trust parameter) and can be used reliably.

For an overview example relating to data restrictions, system 100 can add one or more parameters to data associated with a network (e.g., a proprietary database) for restricted access as a function of the location of the device seeking the information, or a combination of user and location information. For example, system 100 may be programmed to deny access to corporate business information upon request from a network entry device, or coming through an intermediate device that is located outside of a specified region. System 100 also can employ location information to effect a change in a file dependent upon the location of the device accessing that file. In particular, the file may include a lock-out indicator or a destruction indicator if an attempt is made to open it from outside a specified location. One example is sensitive corporate business information. If an attempt is made to access such information from what is otherwise an authenticated device, that information or file may nevertheless be destroyed if the authenticated device is not at a specified location or region. This feature can be seen as valuable in maintaining the security of files retained on or accessed by a device that is not in the possession of an authorized user. The examples that follow describe these overview examples in more detail.

3.2.1 Restricting Access to Network (FIGS. 4 and 5)

As described in the overview example, location information allows system 100 to authenticate and restrict a user based on the location of the device used by the user to access the network. The location information can be added as an authentication attribute to typical authentication systems. Entry into and usage of a network is typically regulated using authentication systems such as Network Operating Systems (NOSs), Remote Authentication Dial-In User Service (RADIUS), described in IETF Request For Comment (RFC) 2138, and IEEE 802.1X standard, which provides for port-based network access control based on a MAC identifier. In the case of NOS and RADIUS, an authentication server (e.g., 142 (FIG. 8))

provides the mechanism for establishing such authentication. In the case of IEEE 802.1X, the network entry devices 114 may be configured with such authentication capability, as described more fully in that standard. IEEE 802.1Q standard provides another means for controlling access and usage of a network. That standard is directed to the establishment and operation of VLANs. The IEEE 802.1Q standard defines the configuration of network devices to permit packet reception at a configured port entry module. Firewalls (e.g., 140 (FIG. 8)) also provide a technique for network usage regulation. Firewalls are primarily computer programs designed to analyze packets and, from that analysis, make a determination as to whether packet transmission into or out of the network is permitted. Being location-aware, system 100 is able to combine the association of a device's physical location with any of these network access regulations as an attribute to assess permitted network access. For example, a VLAN policy template distributed to network devices to configure VLANs can be accompanied by a physical location constraint.

In general overview of the authentication process, a user device 104 connects to the network infrastructure 101, via a connection point 160. System 100 authenticates the device. System 100 receives the location of the device 104 from the device 104 itself and/or from infrastructure 101. System 100 receives user credentials and authenticates the user. During this authentication, system 100 verifies the location of device 104 employing the techniques described herein. If the user is authenticated and the location is both verified and authenticated for the requested network resources, system 100 proceeds in allowing device 104 to access the requested resources. System 100 can log each of these events for administrative use.

To describe this concept in more detail, the following example involves the use of an authentication server (e.g., 142 (FIG. 8)). In this example, the authentication server, utilizing various protocols, such as RADIUS, TACACS+, Diameter, SecureID®, EAP/IEEE 802.1X and/or the like, includes the functionality of a location server. The authentication server/location server also includes a location database. The location database is expanded to support the ability to indicate whether the authentication server should consider location information when a user or network client tries to log in from a certain physical location.

For example, secure military and intelligence environments can require that certain physical locations be protected from unauthorized use of computing systems available in that secure location. Each computing system includes a location client that the computing system employs during the process of authenticating an individual user. The expanded location database

may contain, for example, attributes such as "secure area" or "minimum security level" truth tables. When a user tries to authenticate, the authentication/location server employs the location of the user requesting authorization when validating credentials. The authentication/location server derives this information, for example, using a reference to a connection point ID as described above. If the user has a security clearance of a high enough level to authenticate from that location, the authentication process proceeds. If the user fails to meet the security level associated that particular location, then the network can halt the authentication process, sound alarms and/or report the location of the unauthorized user.

In more detail, FIG. 4 illustrates an example process 401 that system 100 employs to determine whether any restrictions to access the network, based on location, are applicable. Specifically, in example location identification process 401 represented by FIG. 4, a user seeking access to system 100 can be first authenticated (step 405) or otherwise filtered by system 100. System 100 achieves this portion of the authorization process by requiring the end user at a location client device to supply certain user information including but not limited to, a name and one or more passwords (e.g., necessary user credentials). If the user is permitted access to system 100 on that basis (e.g., user name and password), system 100 permits the user to query (step 410) system 100 for access to certain information, applications, and the like. Alternatively or in addition, system 100 receives (step 415) the device location before allowing the requested access. A trusted user device (e.g., 104), a network infrastructure device (e.g., a network entry device 114) and/or a location server can supply the user device location using the techniques as described herein.

With the received location information, system 100 authenticates (step 420) that the physical location of the client device is in a permitted and authorized location for access to the requested network resources. In one example, system 100 permits requested access from devices having pre-approved location identifying equipment, such as a trusted device that can identify the location of that client device. As described above, this can include a GPS receiver associated with the client device that system 100 has previously evaluated for trustworthiness (e.g., cannot provide false location). This also can include a trusted device within network infrastructure 101 such as an authenticated router or switch or a hardwired GPS receiver that can provide location information using the techniques described above. The creation of the trusted device also may

be a recursive function if the client device is located relative to the trusted device and the network or the network location resolution is built outwardly.

In general, system 100 performs an ongoing policing function, for example by repeating the process shown in Fig. 4 periodically or when new information becomes available or triggered by external events.

In another example, the system 100 employs a level of trust parameter to authenticate (step 420) the trustworthiness of the location information. The values for the level of trust parameter can vary, using a sufficiently large scale and range to allow for changes and growth. For example using a sixteen bit word, system 100 can use a a scale from 256 to 3,840, where 256 corresponds to the lowest level of trust and 3,840 corresponds to the highest level of trust. This range, because it does not use all sixteen bits, provides room for growth in the range as system 100 develops over time. Any levels in between the lowest and highest levels of trust represent a mixed level of trustworthiness and system 100 determines whether it will employ the location information with a mixed level dependent on the type of access the user requests (e.g., results of the query (step 410)). A more sensitive application and/or information may require a trust level of 3,072 or greater, whereas a general application and/or information may require a trust level of 1,023 or greater. System 100 may allow a user to access public information regardless of the value of level of trust. In other words, the required level of trust value to authenticate the location can vary depending on the types of resources to which the client requests access.

In one example, system 100 determines the level of trust of the location information based on the originator of the location information. If the location information originates from an internal routing device within infrastructure 101, without public access and under control of a network administrator, and the connection point is a jack in the wall, with an attaching cable that cannot be altered without destroying the wall, the system 100 can assign the highest level of trust value of 3,840 (i.e., this example employs a scale of 256 to 3,840). In this case the probability that the location information will be incorrect or has been altered is very low or non-existent. If the location information originates from a wireless access point (e.g., 120b) within the system 100 that determines the location of the user device using a technique described above, there is some trust because a wireless access point 120 is within the infrastructure 101 of the network. There is some possibility of signal manipulation, however, so system 100 assigns the location

information a level of trust a value of 2,256 because the probability of incorrect location information is relatively higher than the jack in the wall example above. If the location information originates from the user device itself using a system that is allegedly tamperproof, or comes with a third party certification, system 100 can trust this slightly, but again is not sure of what can be done to manipulate signals, so system 100 assigns this a level of trust value of 1,023. If the location information originates from the device with little or no safe-guards (e.g., using a built-in GPS with no tamper-proof technology), system 100 can assign the location information a level of trust of value of 456 (e.g., trusts all GPS signals slightly) or 256 (e.g., no mechanisms to prevent signal tampering, so assign lowest value).

With reference to FIG. 4, once system 100 has authenticated (step 405) the user and authenticated (step 420) the device location information, system 100 considers the access request. System 100 determines (step 425) whether the user has the proper credentials for the level of the requested service. To do this, system 100 compares the user credentials, the location information, and the conditions of access requested (e.g., a request for a certain database of information, a request for a certain application, and the like) with any stored location restrictions. If system 100 determines (step 425) the user is authenticated for the particular request, system 100 determines (step 430) whether the device used by the user is in a location approved or otherwise permitted to receive the requested information, application, and the like. If both threshold questions (step 425 and step 430) are answered in the affirmative, system 100 permits the user to access, via the client device at the known location, the material requested. If either threshold question (step 425 and step 430) is answered in the negative, system 100 denies (step 440) the user access and can notify the network manager. In addition or as an alternative to denying access, system 100 also can entertain, honeypot, and/or otherwise disable and delay the requesting client to provide time for an administrator to take additional action, such as notifying authorities. In another example, system 100 bases access to the requested material solely on device location, and the optional steps of authenticating (step 405 and step 425) based on user identification information are not a pre-condition for access. As described above, system 100 can continually police location authentication by looping steps 415, 420, 425, 430, and 435, as indicated by arrow 440.

FIG. 5 represents another example authentication process 500. In the illustrated process 500, system 100 obtains (step 505) the location information for an client device. In this case,

system 100 employs only the location of the device in determining the appropriate level of service. In another example, system 100 can also employ the user credentials (e.g., user name and password), in addition to the location, to determine the appropriate level of service. System 100 determines (step 510) whether the obtained location is verified. If system 100 determines (step 510) that the location is not verified, system 100 denies (step 515) access or restricts (step 515) access according to predefined policies (e.g., deny any access or restrict access to only those devices, applications and data available to the general public regardless of location). If system 100 determines (step 510) that the location is verified, system 100 determines (step 520) whether the location is authenticated. If system 100 determines (step 520) that the location is not authenticated, system 100 determines (step 525) whether to accept the asserted location. If system 100 determines (step 525) to not accept the asserted location, system 100 denies/restricts (step 515) access according to predefined policies. If system 100 determines (step 525) to accept the asserted location, system 100 allows (step 530) access at selectable service levels, as described below, according to predefined policies.

If system 100 determines (step 520) that the location is authenticated, system 100 determines (step 535) whether the user location is authenticated at the level required. This can include, for example, having a minimum level of trust for the requested level of access. If system 100 determines (step 535) that the user location is not authenticated at the level required, system 100 allows (step 530) access at selectable service levels, as described below, according to predefined policies. If system 100 determines (step 535) that the user location is authenticated at the level required, system 100 allows (step 540) access at the authenticated level.

As described in conjunction with process 500, system 100 allows a user access to system 100 at selectable service levels, based on location information (e.g., step 530). Examples of selectable service levels include, but are not limited to: access denied; threshold access permitted regardless of device location; trusted user and device location is verified but not authenticated, some restricted services permitted; general location verified (e.g., in a public area, airport, country, city, telephone area code or exchange) and some limited access permitted; verified ISP and user verified; verified ISP and user not verified, some limited access permitted; previously authenticated location, re-authentication required based on time intervals; authenticated location and user, permit all predefined permissions; and re-authentication required. Some of these levels can be combined to include additional service levels. For example, re-authentication may be

required at any time for any reason including, but not limited to, topology changes, timeouts, untrusted network devices, location database changes, disconnected cables or local or remote triggers from intrusion detection systems and firewall systems. System 100 can enforce such re-authentication policies, for example by using the edge policing described in FIG. 3. These service levels may correspond to the levels of trust described above (e.g., level of service dependent on a minimum value of the level of trust of the location information).

Use of the above techniques enables system 100 to restrict access to data, applications, specific networked devices, data and network service, QOS (Quality of Service) levels, network tools, functionality, rules, and the like, based on the user and/or the location of the device associated with the user seeking access. Further to the techniques above, system 100 can employ the location information to effect a modification of the access requirements. For example, when a device seeks network access from a location deemed not to be inherently secure (e.g., such as a public facility like an airport), system 100 can prompt a user to initiate an improved connection, such as a virtual private network (VPN), or can inform the user that supplemental restrictions apply while in the insecure area. More generally, this can be seen as an expansion of policy-based access in that the access rules for an individual user may be adapted as a function of the client device location and/or the level of trust associated with the location information.

Further to the techniques described above, system 100 also can provide restricted access to the network based on a particular port connected to the connection point to which the location client is connected. In one example, system 100 employs the techniques above to determine the location of the connection point associated with that particular port, rather than assume a location supplied by the location client is correct. For that particular port for which location has been established and can be trusted, system 100 encodes transmitted data such that the port associated with the trusted location and only that port will accept the encoded data for transmission. If the user disassociates from that particular port, whether intentionally or unintentionally, he/she must re-authenticate.

In this example, system 100 performs the authentication and any re-authentication using an encryption key process. Specifically, an end user, that system 100 has authenticated by user and by location, is provided with an encryption key that is designed to work only on the port through which the key was supplied, and no other. That is, the key cannot be obtained and then used through a different port, which would be the case if the device used by the user were to

move locations (e.g., change connection points). It is to be noted that the key may be tumbled, rotated, and the like. In one example, the network entry device has no knowledge of the specific key, but instead uses the port number/logical port number and one or more of a MAC address, an IP address, its own generated encryption key, and the like, to permit transmission. System 100 also can modify a data packet so that its receiver can only determine whether the transmission came from the right user (e.g., based on the use of the right key) and was modified by an authenticated device (e.g., the location/authentication server) for that particular access port (e.g., 113 (FIG. 1)) of the network entry device (e.g., 114a (FIG. 1)). In another example, there is a three way keying. The client device, the port from the network entry device and the server providing the data each have their own associated keys. In this way, the server can verify that the data coming from the client is indeed coming through the port with the assigned key, for example by verifying signatures on the data from both the client and the authenticated port. In summary, the key is only good for that port which has been specifically established to authenticate that user at the authenticated location. In that way, system 100 can prevent a user from obtaining access, using a false allowable location, by denial of port access when the end user's location has changed, even if the original encryption key for that allowable location has been acquired.

4.2.1 Restricting Location of Data (FIG. 6)

In addition to access control, system 100 can use location information to enforce restrictions regarding the transmission of data. As described in the overview example, location information allows system 100 to deny access to certain sensitive information upon request from a location client outside of a specified region, or to prohibit data from being transmitted through an intermediate device that is located outside of a specified region. FIG. 6 illustrates an example process 601 that system 100 employs to effect these data transmission restrictions. Specifically, in the example information tagging process 601 represented by FIG. 6, system 100 receives (step 605) a request from an end user for access to information (e.g., file, document, and/or the like, generally, data). This assumes that the end user has been adequately authenticated or otherwise permitted access to the network, as described above. System 100 then determines (step 610) whether the requested data is location sensitive. That is, whether the data should not be moved

beyond certain defined boundaries (e.g., a present device, a room, a building, a campus, a city, a country and the like). If system 100 determines (step 610) that the data is not location sensitive, system 100 permits (step 615) access to that data that is not restricted by location.

If system 100 determines (step 610) that the data is location sensitive, system 100 tags (step 620) the data. For example, the application generating the data and/or the server generating a data packet to transport the data over the network can add this tag while generating the data and/or packet. In one example, the tag comprises a file header that identifies location restrictions. The file header also can include a key. In some examples, an end user can request to add a tag to sensitive data such that it cannot be transmitted outside of a defined location (e.g., home, corner office, the courtroom, a hospital, a healthcare facility and the like). The tag may be configured either to deny opening (step 620a) of the transmitted data at an unauthorized location, or to destroy (step 620b) the data when it is determined that the data is in an unauthorized location. The file header may itself be coded or encrypted. Additionally the data/file may be so encrypted such that the deletion of this special file header will either deny opening of the transmitted data, or force the destruction of the data, regardless of the location.

A device within system 100 and/or the data itself determines (step 625) whether the data is outside the permitted location(s). If the data is not outside the permitted location(s), the system 100 permits (step 615) access to the data. If the data is outside the permitted location(s), system 100 denies (step 630) access to and/or destroys (step 630) the data. If the data is going to be routed in the next hop to a location that is outside the permitted location(s), the system 100 prohibits the data from being transmitted to that device outside of the permitted location(s). For example, system 100 can employ edge policing, as described with FIG. 3, where devices of infrastructure 101 police and enforce access by controlling whether or not the data is forwarded to a location client requesting the data. The data itself, or an application trying to access the data, can also police and enforce these restrictions by including executables that obtain the location, with an acceptable level of trust, of the device in which it executes and prohibit access if such location is a prohibited location.

The system 100 can be optionally configured to provide additional security override controls to the end user to prevent destruction of the tagged data or denial of access to the tagged data if the user is located outside of the permitted area of access. In this case, system 100 polices access to the data and not necessarily where system 100 forwards the data. In this example, even

if the data is outside the permitted location(s), the system 100 determines (step 635) whether the tag can be overridden. If the tag can be overridden, the system 100 permits (step 615) access to the data. In this case, the access (step 615) is limited access. For example, the user may be allowed to load the data into a user device for transport, but the user cannot read or edit the data until the user device is located in a permitted location.

4.3 Providing Other Services (FIG. 7)

With a location-aware infrastructure, system 100 can employ trusted location information to provide other services in addition to those described above. For example, system 100 can use the location information in emergency situations, where a device may be an alarm or sensor. System 100 determines the location of the alarm device and transmits the location information to a party responding to the alarm. System 100 can also use location information to recover a stolen user device 104. As the stolen user device 104 accesses system 100, system 100 determines the location of the stolen device and transmits the location information to a party seeking to locate the device. System 100 can track mobile user devices (e.g., 104b) and thus can also track anything associated with that user device (e.g., the user, a file, a physical object, and the like). System 100, through the use of location information, can provide these and other services and applications. The examples that follow illustrate how system 100 can employ location information to provide these and other services and applications.

In one example, FIG. 7 illustrates a process 700 for establishing a security service in a network environment based on location information. In process 700, the client devices may be physical intrusion detection devices, smoke detectors, fire alarms, EMT devices, wireless panic buttons, and the like. These client devices are designed to signal an emergency event. Alternatively, the device may be any sort of network-connected device that is configured to transmit an alarm upon failure or imminent failure, or to transmit an alarm if a device connected to it fails. If the device includes a location module 185, location server 134 can provide and store that device's location information in that device itself.

In one example, an event triggers (step 705) a smoke detector on the 4th floor of the 5th building on the left side of the street. System 100, to which the triggered device is connected, either determines the device's location using the techniques described herein or queries (step

710) the triggered device's specific location information. System 100 directs the query to the device itself, or to location server 134. System 100 receives (step 715) the location information, either as an absolute or a relative location. As described above, the location information may or may not be trustworthy. System 100 can verify the location information to make it trustworthy or increase the level of trust required for the particular security service system 100 is providing. System 100 relays (step 720) that detailed location information to the appropriate authorities, potentially leading to greater response efficiencies. A location client having a network association can be made more effective by linking the device's location information with that device's operation.

Another example of a security service system 100 provides is to protect sensitive devices from theft. For example, if a laptop computer is stolen and the thief seeks to access system 100, system 100 evaluates the location information, whether obtained directly from that client or from the location server 134 when the end user accesses the network. In the event that network entry is sought, the location of the requesting client is acquired. Assuming system 100 can determine that that particular location client has been stolen, system 100 supplies the location information to a suitable authority. To provide authorities enough time to get to the identified location, system 100 also can entertain, honeypot, and/or otherwise disable and delay the requesting location client. The location-aware system 100 thus can be used as an effective means to exchange accurate location information in relation to a security violation and, potentially, to neutralize effects associated with that violation.

Yet further, the location-based system 100 and the techniques described herein may be employed to regulate and/or accurately monitor the movement of individuals, equipment, packages, and the like, as they travel near and through network infrastructure 101. An electronic device (e.g., user device) that communicates with system 100 is applied to a pass, a label, an asset tag, and the like. That device includes means to enable tracking of its location using techniques, for example, the radio-based techniques described above. For example, all visitors to a secure facility are supplied with a visitor pass. That visitor pass includes a transceiver that is capable of communication with wireless access points (e.g., 120b (FIG. 1)) of network infrastructure 101 positioned throughout the facility. These wireless access points can be configured such that as the tag/pass/visitor moves throughout the facility, network infrastructure 101 determines the visitor's location using the techniques described above. In addition, security

guards can know whether any visitors remain in the facility at a planned closing time. This eliminates the need for the facility to maintain a separate tracking system with sensors. Instead of the separate tracking system, the same data network infrastructure 101 employed for network access also can be employed for tracking, by associating a location with each of the devices that communicate with network infrastructure 101.

These techniques enhance network security, enhance device security, likely improve emergency responsiveness, and may be employed to establish network-based organizational security. These and many other advantages are provided through the association of relevant network device and networked device location information with security, protection, and response efforts. System 100 can also provide other services based on location not described above. For example, system 100 can provide enhanced network topology discovery and mapping, with device map representations specific to their physical location. For example, system 100 can employ location information to prepare accurate maps that associate devices with their physical locations. System 100 also can provide device inventories by location, without the need of manually verifying each device individually. As described above, the location database can be expanded to include device ID information along with the corresponding location information.

Further, system 100 can employ location information to check that network rules are followed (e.g., if wiring designs are inaccurate and must be supplemented or changed). The location information can be of value to the LAN manager and, for example, to an Internet Service Provider (ISP) or a cable operator interested in knowing the locations of cable modems and phone line terminations.

System 100 also can provide information to a user that is relevant based on that user's current location. For example, a traveling end user may dial into the network, have the connecting device's location information acquired or supplied, and then be directed to hotels, restaurants, and the like, within a defined radius of the device's location and meeting any number of selectable criteria.

5.0 Some Additional Examples (FIG. 8)

Referring to FIG. 8, system 100' provides another example of a location-aware network and is described as an enterprise network that serves as a data communications network for a business organization or other type of enterprise. The enterprise operates the network according to various policies, which may include location-dependent aspects. For example, access-control policies may depend on the locations of devices accessing services on the network. In various configurations, system 100' may include or make use of one or more LANs, MANs, WANs, PANs and/or Ethernet to the first mile (e.g., IEEE 802.3ah). In other examples of such a network, the physical and logical arrangement of the devices can differ from that shown in FIGS. 1 and 8.

System 100' includes various types of devices. Some devices are network entry devices 114c-j, generally 114, which provide access to an infrastructure 101' of system 100' to user devices 104c-l, generally 104, or to external networks such as Internet 148 or telephone network 132. The portion of system 100' excluding user devices 104 and external networks is referred to as network infrastructure 101'. This infrastructure 101' includes devices for switching and routing data within the system 100', including one or more central switching devices 136' and computers that provide services in support of access to and routing of data in the system 100', including an authentication server 142, an application server 134', and other servers such as a domain name server (not shown). In addition, system 100' includes devices such as a printer 122 and a fax machine 123 which have some characteristics of both user devices and of network infrastructure devices.

Network entry devices 114 provide access to network infrastructure 101' over various types of transmission media, including cable-based or wireless. The cable-based transmission medium can include, for example, twisted pair wires used for a 100-Base-T Ethernet link. A cable-based transmission medium can also be a shared cable-based transmission medium that can connect more than two devices. For example, a coaxial cable used for 10-Base-2 Ethernet, telephone cables used for high-frequency (e.g., HomePNA) communication between multiple devices, and power lines used for data communication (e.g., HomePlug) between devices provide such shared cable-based transmission media.

Entry devices 114 together include a number of entry port modules (e.g., 113' and 118), each associated with a different medium (e.g., a cable and/or a portion of a radio spectrum). For instance, in system 100', entry port module 113' of network entry device 114f is connected to user device 104c by a dedicated cable-based transmission medium 112'. Entry port module 118 of network entry device 114g is connected to user devices 104d-f by a shared wireless transmission medium 119'. Entry port module 146 of network entry device 114d is connected to user device 104g by Internet 148 and shared transmission medium 152. Further, entry port modules 126, 128, and 130 of network entry device 114e may be connected to user device 104h by telephone network 132 and by shared transmission media 154. Entry port modules 126, 128, and 130 of network entry device 114e may also be connected to user device 104m using a cellular telephone (or PCS) tower 175, which is connected via a base station 178 to the telephone network 132 and the shared transmission media 154. Any of network entry devices 114 may be coupled by different port modules to both shared and dedicated transmission media as well as cable-based and wireless transmission media.

Network entry devices 114 and end user devices 104 can come in a wide array of configurations. For example, user devices 104 can include individual computers, printers, servers, cellular phones, laptops, handheld electronic devices, telephones, Internet Protocol (IP)-configured telephones, switch devices, and the like. Network entry devices 114 can include, for example, switches, routers, hubs, bridges, repeaters, wireless access points, data communications equipment, server computers, modems, multiplexers, Private Branch Exchanges (PBXs), virtually any devices used to interconnect data equipment or end devices, and the like. The discreet boundaries of infrastructure 101' are for illustration only. For example, system 100' may include a server outside of the illustrated boundary while remaining logically part of infrastructure 101'. In another example, there may be a portion of network infrastructure 101' connected to system 100' located in a remote network, such as Internet 148.

In any particular physical arrangement of system 100', each device (e.g., 104, 114) has a connection point (e.g., 160c, 160d, 160e, 160f, and 160g, generally 160). A connection point 160 is the place where an associated device connects to system 100', and thus corresponds to the location of that device. For example, for devices communicating via a cable (e.g., 104c, 104g, 104h, and 114g), their connection points (e.g., 160o, 160l and 160k, and 160n, respectively) represent the terminus of the cable (e.g., a wall jack) where the respective devices physically

attach to make a connection to the network. For example, connection point 160o represents the terminus of cable 112'. For wireless device 104f, the transmission medium is air, so the respective connection point 160m represents the location of the receiver antenna receiving signals from the wireless device. For any physical arrangement of system 100', each connection point 160 is associated with a connection port in network infrastructure 101' that provides connectivity to the rest of system 100'. For example, user device 104c, which is attached to connection point 160o (at the end of medium 112'), is associated with connection port 113'. Note that should the physical arrangement of system 100' change, for example, if medium 112' were disconnected from port 113' and reconnected to a different port in the same device or in a different device, the association of a connection point and a connection port may change. As described above, maintaining an association of connection points and connection ports, particularly in generating connection point IDs, provides a way for determining locations of devices in the system 100'.

5.1 Distributed Location Database

In some of the techniques/mechanisms described above, system 100 employs a centralized location server 134 that contained location server functionality and the location database. As an alternative to the centralized system, the location-aware portion of system 100 can be implemented as a distributed system. In examples of a distributed system, the location server functionality and the location database are distributed among the devices of the network. In example distributed systems, location module 185 exists in any one, a portion, or all of the exemplar devices of a network, including for example the entry devices (e.g., 114), a server (e.g., 142), a firewall (e.g., 140), and the like. As illustrated in FIGS. 1 and 8, some devices comprise a location module (e.g., 185a-o, generally 185), whether in hardware, firmware, or software, that can be configured to include different functionality and pieces of information, including location information. As described below, for a distributed system example, devices both inside and outside network infrastructure 101 can optionally maintain location dependent information that affects their operation.

5.1.1 Distributed Within the Network

FIGS. 1 and 8 illustrate location modules 185 in a portion of the devices for example only. As described above, the information representing the location of a particular network device, or one or more devices attached to a particular network device, may be preloaded into location module 185 as a database. The location database at each device can be the entire location database of system 100, or a portion of the location database. In particular, the portion of the database included in the location module 185 of the device can be a portion with those locations applicable to that particular device. For example, all of the connection points associated with the ports of a particular network entry device. Alternatively, location module 185 may include an updateable table that changes with additions or deletions to system 100 and/or movement of devices associated with system 100. Location module 185 can include location information and can be configured to measure, calculate, infer, search, and/or otherwise acquire information to provide one or more of the detailed mechanisms/techniques described herein. Location module 185 also can be configured to be an access control module that enables regulation (e.g., policing) of access to network-based data, applications, QoS, ToS, bandwidth, and the like, based on device location information. For example as illustrated in FIG. 4, for the distributed system, location modules 185 are configured to include device location as a requirement to permit access to network-based information, applications, rate service, rate type, and the like. With such a distributed system, each network entry device (e.g., 114) becomes a quasi-authentication server. As illustrated in FIG. 6, location modules 185 are configured to include means for tagging location-sensitive information/data and acting on that tag accordingly. Each location module 185 also can enable identification of the location of a communicating device for the purpose of providing security, safety, or other services described above.

For the distributed example, location server functionality can be part of any network device, management station, or server/authentication server. The location server functionality may be co-located within a switch or network device (e.g., 114) through which a user device communicates. In a distributed system, devices can include functionality in their respective location modules 185 to be both a location client and a location server. In remote offices, a router that connects the remote office to the home office can comprise the location server functionality, as it may need to provide location information for E911 applications, for example.

In other applications, such as an enterprise campus networks, the location server functionality may be part of an enhanced IP address management system such as a Dynamic Host Configuration Protocol (DHCP) server as well as a dedicated location provisioning system.

The following is a list of a few possible devices (but not limited to only those devices) that can contain the location server functionality: network switches, data switches, routers, firewalls, gateways, computing devices such as network file server or dedicated location servers, management stations, network connected voice over IP/voice over data systems such as hybrid PBXs and VoIP call managers, network layer address configuration/system configuration servers such as enhanced DHCP servers, enhanced Bootstrap Protocol (bootp) servers, IPv6 address auto-discovery enabled routers, and network based authentication servers providing services such as radius, extensible authentication protocol/IEEE 802.1X or others.

In one example, to provide the distributed location databases with location information, system 100 employs a Simple Network Management Protocol (SNMP). A network administrator provisions the location information of the terminus of a network cable in the SNMP ifDescr variable (e.g., the ifDescr is a read only attribute, but many systems allow a network operator to "name" a port which then will be displayed in this field). The location server functionality of a device reads the terminus information via the SNMP.

As described above, the location client attempts to learn its geographic location and/or identifies itself to another device with a need to know the client 's location. An advanced location client can also receive its operational configuration from a location aware network (e.g., from a location server configured to additionally provide configuration information). The location client communicates with any network element and discovers its connection point ID through one of many possible methods described herein. Once the location client knows its connection point ID, it can contact a location server to discover its actual location, or to register itself with the location server, which can act as a proxy for other communication entities seeking to discover the location of the location client. It is also possible for a location server to be a communication system that may modify the location client's communication traffic with the device's location information.

The following is a list of a few possible devices (but not limited to) that can contain a location client: network switches, routers, firewalls, gateways, computing devices such as a network file server or end user computing devices, personal digital assistants, smart appliances

(toaster, refrigerator or coffee pot with network connectivity), network connected voice over IP/voice over data systems such as hybrid PBXs and VoIP call managers or voice over IP/data handsets.

5.1.2 Distributed Outside of the Network

In addition to their being distributed among the devices of system 100, system 100 can employ location information from a trusted database that is external to the network and/or a trusted database maintained by a third-party. As described above, system 100 can assign a level of trust for all of the location information obtained from a database external to system 100. For example, in the telephone network example, where the unique connection point ID can be a telephone number, the location server functionality, either in location server 134 or any of the distributed functionality in the location modules 185, can reference a white-pages type database to retrieve an address for the telephone number. If the address is not a location format recognized by a location-aware application, the location server functionality can reference another third-party database to convert the address to latitude and longitude coordinates, for example. Further granularity may be obtained. For example, for a home business, an address may have two phone numbers associated with it, a business phone number and a residential phone number. The location of the connection point identified with the business phone number is in the room established as the home office. This may be located on one floor of the house, providing altitude coordinates also. The location of the connection point identified with the residential phone number is in the room containing the family personal computer. This may be located on another floor of the house. Similarly, the location server functionality can obtain an address, a room, and/or geographical coordinates where the connection point is a cable endpoint connected to a cable modem and the IP address is associated with an address of the subscriber. System 100 can use any available resources to update the location information of particular connection points, assigning the appropriate level of trust based on the trustworthiness of that third party source.

5.2 Use of a Location Advertising System in a Distributed Network

In one distributed example, system 100 employs a location advertising system to communicate information among the devices. A location advertising system comprises a networking device that provisions and/or advertises device location information and/or configurations to a location client device over the network, typically using a layer 2 or layer 3 protocol (e.g., a neighbor discovery protocol). The location advertising system also comprises devices to which location client devices may connect via the network. An example of a location advertising system device can include a location advertising switch, which is a device, such as a data switch operating as a layer 2 or layer 3 LAN switch. Another example of a location advertising system device can include a location advertising router, referred to sometimes as an automated configuration server, which comprises a network router. This device can also comprise a branch office router that can provide a configuration to a LAN switch and/or a wireless access point in a remote enterprise office. Other devices in the location advertising system can include a wireless LAN access point, a virtual private network system, a tunnel server, a remote client, a gateway and/or the like. A device acting as a location advertising system may distribute location information based on various coordinate systems or textual representations of a physical location. A device in the location advertising system, when it is a device that has location clients physically connected to it via physical cables, contains a database of connection points that correspond to a physical network access port and the corresponding geographic location information of the terminus of the network cable connected to that port, similarly as described above. Although presented in the context of a distributed system, the location advertising system can also be implemented in a centralized system using a centralized location server as described above.

When system 100 employs a LAN Switch in its location advertising system, system 100 not only provides location and configuration information to a location client device, but it also can automatically map network policies to the port where the location client device is connected. This policy may be provisioned on the location advertising switch as soon as the location client is detected or policy provisioning may be enabled only after the location client is properly configured and verified. This feature is referred to as self-enabled policy.

When a location advertising system comprises a wireless LAN access point, the network maps location and configuration information to a device specific identification, IEEE MAC address as an example, and the IEEE 802.11 association ID present during the operation of the

wireless network. The network maps the location coordinates to the association ID. As wireless networks afford client devices total mobility, the system employs techniques, such as the techniques described above for example, to triangulate the coordinates of the location client at any instance. The location database can be dynamic in nature as the client's coordinates can potentially change very frequently.

5.2.1 Specific Examples Using a Location Advertising System

One example of automated network management employing the location advertising system is the configuration of Voice over IP handsets with a neighbor discovery protocol in a data network. Voice over IP handsets typically are designed to communicate with Ethernet switches and can require complex configurations. Networks with the location advertising system can integrate neighbor discovery protocols with Voice over IP handsets to provide configuration information to the handset, discover inventory information to be stored on the connection point switch, and automatically configure the ports' parameters on the connection point switch/access platform.

The automated voice handset configuration system in this example can provide the voice handset with several parameters. For example, the system can provide VLAN membership and classification rules for voice and/or fax payload and control traffic. The system can also provide VLAN membership and classification rules for non-voice payload and control traffic. The system can also provide the IEEE 802.1Q prioritization packet marking information of voice payload and control traffic. The system can also provide the IEEE 802.1Q prioritization packet marking of non-voice payload and control traffic. The system can also provide the IP type of service field markings for the voice payload traffic. The system can also provide the IP type of service field marking for fax payload traffic. The system can also provide the IP type of service field marking for voice/fax control traffic. The system can also provide the Internet address for the voice entity contained in the VoIP phone. The system can also provide the ANSI LIN (Location Identification Number). The system can also provide the geographic location of the handset with geodesic information or any other geographical coordinate system including elevation or relative location information.

For illustration of this specific example, let user device 104c (FIG. 8) represent a VoIP handset and network entity device 114f represents a LAN switch. The LAN switch 114f includes location advertising system functionality, for example, as part of location module 185n. The LAN switch 114f also includes an expanded database in location module 185 that includes inventory information, geographic information and configuration information. In operation, the Voice over IP handset 104c boots and starts sending out neighbor discover protocol packets. These packets trigger the LAN switch 114f to which the VoIP handset 104c connects to start sending neighbor discovery protocol packets. The LAN switch 114f responds back to the voice handset 104c with the following configuration information obtained from its expanded database: IEEE 802.1Q priority marking configuration, IEEE 802.1Q VLAN membership configuration rules, Internet protocol type of service/differentiated services marking rules, the IP address of the voice call managers/IP PBX/IP voice switch which the voice handset 104c needs for normal operation, and the ANSI LIN. The LAN Switch 114f enables policy management configurations on the port where the switch connects (e.g., self enabled policy). The voice handset 104c continues to utilize the neighbor discovery protocol to continue to advertise its device specific information. This device specific information can include, for example, model number, device type, IP address, device serial number, microcode version utilized by the handset, and the like. The LAN switch 114f decodes this device specific information from the neighbor discovery protocol packets sent by the voice handset 104c and records the advertised information to a local or remote network management database. The system 100' uses this information to support inventory management and device location applications.

Another specific example of automated network management employing the location advertising system involves the use of network LAN switches in a campus or enterprise network as a vehicle to configure wiring closet switches or wireless access points. In many enterprise networks, the IT organization spends a great deal of time and resources configuring access switches or wireless LAN access points that act as the primary network entry device for network users. These network entry devices normally are provisioned with simple configurations, but occasionally a minor misconfiguration can cause many problems in the operation of a data network. A network with the location advertising system frees network administrators from worrying about the validity of network devices as backbone network switches provision network

access switches and routers with the appropriate configuration based on where they connect to the network.

For illustration of this specific example, let network entry device 114f (FIG. 8) represent a wiring closet or a user access switch acting as a configuration client. In this environment, the user switch 114f is configured to participate as a location client (e.g., includes location client functionality in location module 185n). The location client 114f is connected to network infrastructure 101' via connections to network entry device 114c, network entry device 114g, and central switching device 136'. Any of those other devices (i.e., network entry device 114c, network entry device 114g and central switching device 136') can act as a location advertising system switch and broadcast location, configuration, and other information to the network entry device 114f, in this example, the location client.

To determine its physical location, device 114f receives location information from each of its neighboring devices, 114c, 114g, and 136'. Device 114c determines that since neighboring device 114f is connected to connection point 160u, device 114c is located at location X1, Y1 and transmits the location information to device 114f. Similarly, device 114g determines that since neighboring device 114f is connected to connection point 160v, device 114c is located at location X2, Y2 and device 136' determines that since neighboring device 114f is connected to connection point 160w, device 114c is located at location X3, Y3. Device 114c receives the coordinates from each of its neighboring and compares them with each other to determine, with a statistical level of confidence what its actual physical location is. This level of confidence can be translated into a level of trust to associate with the calculated physical location based on the received data. For example, if all three neighboring devices provide the same coordinates, then system 100' can associate the highest value for the level of trust with that physical location.

To determine configuration, any combination of the other devices (i.e., network entry device 114c, network entry device 114g, and central switching device 136') advertises configuration parameters to location client 114f. The configuration parameters can include, for example, the following attributes: IP address of the user access switch, IP subnet mask of the user access switch, default IP route of the user access switch, SNMP trap destination IP address, SNMP read only community string, SNMP read-write community string, default VLAN ID on user ports, default IEEE priority mark for user access traffic, IEEE 802.1D spanning tree enabled or disabled, IEEE 802.1W rapid spanning tree enable or disable, enable IEEE 802.1X

authentication on user ports, enable IEEE 802.1Q VLAN tagging on ports to data center/configuration provisioning switch, geographic coordinates of the terminus of the data cable connected to this port, and the like. Table 4 illustrates an example of some entries that can be included in an expanded location database in this location advertising system example. In this example, the first five columns from the left (i.e., entry port to geographic location, inclusive) represent information provisioned on the location client. The last two columns from the left (i.e., client switch IP address and serial number) represent information obtained/learned from the location client.

Entry Port	Default VLAN ID on User Ports	Default Priority	Enable Tagging on the Port where location data is Received	Geographic Location of Cable Terminus	Client Switch IP Address	Serial Number
1	1024	0	TRUE	Lat X1, Long Y1, Alt Z1	1.1.2.1	xxxxxx1
2	1024	0	TRUE	Lat X2, Long Y2, Alt Z2	1.1.2.2	xxxxxx2
3	1025	0	TRUE	Lat X3, Long Y3, Alt Z3	1.1.3.1	xxxxxx3
4	1026	0	TRUE	Lat X1, Long Y4, Alt Z4	1.1.4.1	xxxxxx4

Table 4

It is also possible for the location advertising system in the provisioning switch to provide a temporary Internet address and/or the unified resource locator (URL) to a network attached location database where the location client can retrieve a more advanced configuration file. For example, see entries 6, 8, and 10 of Table 3 above. The configuration file can be retrieved via standard mechanisms such as trivial file transfer protocol or Internet file transfer protocol.

Another specific example of automated network management employing the location advertising system is the provisioning of a basic switch configuration for local and wide area routers in a branch office. In this example, the network employs a branch office router and a regional office as part of its location advertising system. In one example of the operation described below, the user access switch is a branch office router and the data center switch is a regional office router. In another example of the operation described below, the user access

switch is a network entry device in the branch office and the data center switch is a branch office router.

In operation, a user access LAN switch boots and starts sending out neighbor discover protocol packets. These packets will trigger the data center LAN switch/location advertising switch to which the location client connects to start sending neighbor discovery protocol packets. The data center switch/location advertising switch advertises the configuration associated with the port to which the location client/user access switch connects. This enables policy management configurations on the port to which the switch connects (e.g., self enabled policy). The user access switch continues to transmit neighbor discovery protocol packets to update the data center switch with inventory information, which can be accessed by a network management system.

5.3 Format of Location

The format of location information can vary in different versions of the system. The examples above illustrate some of the formats for location information. The following formats are included as additional examples. The location information may be established as grid or map coordinates on a defined map coordinate system. For example, the location information can be considered absolute (e.g., latitude x by longitude y, GPS location, Loran, Loran C, military grid), regional (e.g., Massachusetts, building 1, the third floor), relative (e.g., x feet from door y on floor z, office five on floor 3, on a 30-degree radial from point A), and/or aircraft systems, such as Very High Frequency (VHF) Omnidirectional Range (VOR) or Emergency Location System (ELS) . It is to be noted that GPS locating would include satellite and ground-based stations. The location information may be three dimensional, including elevation above sea level or above some defined position. The location information can include a fourth dimension, accuracy indicator, as required by the federal communications commission for emergency E911 interoperability. The location information also can include a location identification number as required by the federal communications commission for emergency E911 interoperability. The location information can be typed as numerical, string and the like.

5.4 Communicating Location Information (FIGS. 1 and 8)

To transmit location and other information among devices, the devices can communicate with each other using a variety of protocols, which can be based on the specific network solution considered. The examples above illustrate some of the protocols used to exchange information. The following protocols are included as additional examples. The devices can employ the Internet Protocol (either version 4 or 6). A high layer protocol can be used based on how system 100 distributes the location information. For example, if system 100 stores the location information as tables or files, system 100 can employ a high layer protocol such as Light Weight Directory Access Protocol (LDAP) to access and transmit location information between devices. If system 100 stores the location information as databases, system 100 can employ a high layer protocol such as, Structured Query Language (SQL) or Open Database Connectivity (ODBC) to interact with devices over the Internet Protocol.

The devices also can use a Layer 2 protocol, or a protocol that does not rely on having an IP address to communicate. This enables the devices to define the network layer address, and enables two devices to communicate on networks not operating with the Internet Protocol. The devices can also employ Extensible Authentication Protocol (EAP) or IEEE 802.1X to communicate with each other. The devices can also communicate using proprietary protocols that ride over IP (or other Layer 3 protocols) or MAC layer protocols.

For illustration, an example in the specific examples of locating devices section above employs IEEE Bridge Spanning Tree Protocol. That example can be illustrated using other protocols also. For example, in another example, system 100 employs a proprietary network neighbor discovery protocol, Cabletron Discovery Protocol (CDP) by Enterasys Networks, Inc. of Rochester, New Hampshire. In a CDP example, network devices utilize this protocol to provide neighbor discovery. A CDP discovery packet is sent (step 305 (FIG. 3)) at defined intervals out of all ports with such discovery enabled. The location client receives (step 310 (FIG. 3)) the discovery packets and decodes the device ID field. In a CDP discovery packet in particular, the device ID field is based on the primary switch MAC address with the SNMP ifIndex of the port from which the packet was sent. Using that decoded information, the location client determines (step 315 (FIG. 3)) that the connection point ID={Primary Switch MAC}+{CDP Sourcing Port 's ifIndex}.

The system 100 can employ a combination of protocols to further automate the techniques above. One example employing a combination of protocols is an automated technique that populates the location database, whether centralized or distributed, with connection point IDs. Both the CDP and the IEEE Spanning Tree Protocol have IETF SNMP Management Information Bases (MIB) associated with them. The location server, when enabled with a SNMP client, can generate a list of connection point IDs in the network environment.

In environments where IEEE Spanning Tree Protocol is the mechanism used to discover a location client's connection point ID, the network can use the IETF dot1dBridge MIB. The network uses the dot1dBaseBridgeAddress MIB object to define the unique switch identification. The network can derive the MAC address of the physical port by polling the dot1dBasePortifIndex MIB object. This MIB object corresponds to the ifIndex pointer in the IETF SNMP MIB 2 Interface MIB. By looking up the ifPhysAddress MIB object by knowing the ifIndex, the network management device is able to populate the Connection ID list (e.g., IEEE 802.1D Connection ID=Switch Base MAC Address +Port MAC Address).

When utilizing CDP as the protocol to detect a Connection ID, the network can generate the connection list by polling certain SNMP variables. The network uses the dot1dBaseBridgeAddress MIB object to define the unique switch id. The network derives the MAC address of the physical port by polling the dot1dBasePortifIndex MIB object. This MIB object corresponds to the ifIndex pointer in the IETF SNMP MIB 2 Interface MIB (e.g., CDP Connection ID=Switch Base MAC +ifIndex).

In some examples, it is possible for network switches to store location information for each switch port using SNMP. A voice handset MIB allows the switch to store the ANSI LIN number for each port. This network can provision this information in the switch via SNMP sets or local command line configuration. This network can poll and/or map this information to the connection point ID information.

5.5 Other Miscellaneous Variations

Other variations of the above examples can be implemented. The level of trust in the examples above is described as a discrete numerical value. One example variation is that system 100 can employ string types and fuzzy logic techniques to implement the level of trust. For

example, the levels of trust can be very trustworthy, trustworthy, not too trustworthy, neutral, untrustworthy and very untrustworthy.

Another example variation is that the illustrated processes may include additional steps. Further, the order of the steps illustrated as part of processes is not limited to the order illustrated in their figures, as the steps may be performed in other orders, and one or more steps may be performed in series or in parallel to one or more other steps, or parts thereof. For example, user verification and location verification may be performed in parallel.

Additionally, the processes, steps thereof and various examples and variations of these processes and steps, individually or in combination, may be implemented as a computer program product tangibly as computer-readable signals on a computer-readable medium, for example, a non-volatile recording medium, an integrated circuit memory element, or a combination thereof. Such computer program product may include computer-readable signals tangibly embodied on the computer-readable medium, where such signals define instructions, for example, as part of one or more programs that, as a result of being executed by a computer, instruct the computer to perform one or more processes or acts described herein, and/or various examples, variations and combinations thereof. Such instructions may be written in any of a plurality of programming languages, for example, Java, Visual Basic, C, or C++, Fortran, Pascal, Eiffel, Basic, COBOL, and the like, or any of a variety of combinations thereof. The computer-readable medium on which such instructions are stored may reside on one or more of the components of system 100 described above and may be distributed across one or more such components.

A number of examples to help illustrate the invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

WHAT IS CLAIMED IS:

1. A method of determining a physical location of a client in a data communication network, the method comprising:

determining an identifier of a connection point through which the client communicates with the data network; and

determining a physical location of the client based on the determined identifier of the connection point, including accessing a stored association between the connection point identifier and the physical location.

2. The method of claim 1 wherein the connection point provides a communication path to the client via a cable-based transmission medium.

3. The method of claim 1 wherein determining the physical location is in response to the client connecting to the connection point.

4. The method of claim 1 further comprising storing a plurality of associations of connection point identifiers with respective physical locations, including storing the association between the connection point identifier and the physical location prior to the client connecting to the connection point.

5. The method of claim 1 further comprising transmitting connection information from a network device in the data network to the client, and wherein determining the connection point identifier further comprises determining the connection point identifier using the connection information.

6. The method of claim 5 wherein the network device provides a communication path from the connection point to other devices in the data communication network.

7. The method of claim 5 wherein the connection information comprises a first portion that identifies the network device.

8. The method of claim 7 wherein the first portion comprises an address of the network device.

9. The method of claim 8 wherein the first portion comprises a MAC address of the network device.

10. The method of claim 8 wherein the first portion comprises an Internet Protocol (IP) address of the network device.

11. The method of claim 5 wherein the connection information comprises a second portion that identifies a connection port of the network device that provides a communication path to the connection point.

12. The method of claim 11 where the second portion comprises a MAC address of the connection port that provides the communication path to the connection point.

13. The method of claim 11 where the second portion comprises an index attribute contained in the device ID.

14. The method of claim 1 wherein determining the physical location further comprises:

receiving a signal from the client; and

measuring, by a network device in the data communication network, a first characteristic of the signal.

15. The method of claim 14 wherein determining the physical location further comprises determining the physical location based on the measured first characteristic.

16. The method of claim 14 wherein determining the physical location further comprises:

storing associations of previously measured characteristics with respective physical locations; and

determining the physical location using the measured first characteristic and the previously measured characteristics.

17. The method of claim 14 wherein measuring further comprises:

measuring, by a first network device, the first characteristic of the signal received via a cable-based transmission medium from the client; and

measuring, by a second network device, a second characteristic of a signal received via a wireless transmission medium from the client, and

wherein determining the physical location further comprises determining the physical location using the measured first characteristic and the second measured characteristic.

18. The method of claim 1 further comprising storing the association between the connection point identifier and the physical location using a location database.

19. The method of claim 18 wherein storing the association comprises storing the association between the connection point identifier and the physical location in a centralized location server.

20. The method of claim 18 wherein storing the association comprises storing the association between the connection point identifier and the physical location distributed among network devices.

21. The method of claim 1 wherein the connection point comprises a jack.

22. The method of claim 1 further comprising storing an association between the physical location and at least one of a MAC address, a network layer address, a phone number, a protocol type, an asset ID, and an owner.

23. The method of claim 1 further comprising determining an authentication using the determined physical location.

24. The method of claim 1 further comprising determining a level of service using the determined physical location.

25. The method of claim 1 further comprising employing a security feature that uses the physical location.

26. The method of claim 25 wherein employing the security feature comprises encrypting data based on the physical location.

27. The method of claim 25 wherein employing the security feature comprises employing a temporary key associated with the physical location.

28. The method of claim 1 wherein determining the physical location further comprises:

searching a plurality of stored associations for the determined connection point identifier; and

identifying the physical location associated with the connection point identifier in the stored associations.

29. The method of claim 1 wherein the determined physical location comprises at least one of a latitude and longitude format, a latitude, longitude, altitude, and accuracy format, a location identification number, a textual string representation, and a relative physical location with relationship information.

30. The method of claim 1 further comprising establishing a connection policy using the determined physical location.

31. The method of claim 30 further comprising authenticating a user using the connection policy.

32. The method of claim 1 further comprising transmitting the determined physical location to a device associated with the connection point.

33. The method of claim 1 further comprising transmitting configuration information to a device associated with the connection point based on the physical location.

34. The method of claim 1 wherein determining the physical location further comprises determining, by a trusted device, the physical location based on the connection point.

35. The method of claim 34 wherein the trusted device is located within a network infrastructure.

36. The method of claim 1 further comprising storing an association between the physical location and a trust level.

37. The method of claim 36 further comprising determining the trust level of the physical location using a device that determines the physical location.

38. A method for surveying a data network infrastructure including a plurality of connection points, the method comprising:

for each of a plurality of connection points to the data network infrastructure,

determining a physical location for the connection point, and

providing to the network infrastructure the physical location for said connection point.

39. The method of claim 38 further comprising storing associations between the connection points and their respective determined physical locations.

40. The method of claim 38 further comprising identifying the connection points with respective connection point identifiers.

41. The method of claim 38 further comprising, for at least some of the connection points, connecting a location sensing device to the connection point and determining the physical location of the connection point using the location sensing device.

42. The method of claim 41 wherein the location sensing device comprises a Global Positioning System (GPS) receiver.

43. The method of claim 41 wherein the location sensing device comprises an inertial positioning system.

44. A method of determining a physical location of a client in a data communication network, the method comprising:

connecting the client to a connection point via a cable-based transmission medium;

identifying the connection point with which the client communicates;

determining a physical location of the client based on the identified connection point; and

storing an association between the identified connection point and the determined physical location.

45. A system comprising a location module configured to determine a connection point identifier, to determine a physical location based on the connection point identifier, including accessing a stored association between the connection point identifier and the physical location.

46. The system of claim 45 further comprising a location client in communication with the location module.

47. The system of claim 45 wherein the location client communicates with the location module using a communication protocol.

48. The system of claim 45 wherein the location client communicates with the location module using a layer 3 protocol.

49. A method comprising:

determining, by one or more trusted network devices within a data network infrastructure, a physical location of a client device requesting access to the data network infrastructure to generate a trusted physical location; and

storing an association of the trusted physical location with the client device.

50. The method of claim 49 further comprising determining whether a network device within the data network is a trusted network device according to a likelihood that the network device can be modified to provide false physical location data.

51. The method of claim 49 further comprising limiting physical access to the trusted network devices within the data network.

52. The method of claim 49 wherein the one or more trusted network devices are each associated with a level of trust not less than a threshold.

53. The method of claim 52 wherein the threshold depends on a type of request by the client device.

54. The method of claim 49 wherein the trusted physical location is associated with a level of trust.

55. The method of claim 54 further comprising determining the level of trust of the trusted physical location using levels of trust of the one or more trusted network devices.

56. The method of claim 55 wherein determining the level of trust comprises determining the level of trust based on a method of communication between the one or more trusted network devices and the client device.

57. The method of claim 49 further comprising policing network activities of the client using the trusted physical location.

58. The method of claim 49 further comprising determining a response for an access request by the client using the trusted physical location.

59. The method of claim 49 further comprising controlling network resources provided to the client using the trusted physical location.

60. The method of claim 59 wherein controlling network resources includes restricting access to said network resources.

61. The method of claim 49 further comprising transmitting the trusted physical location to an emergency response authority.

62. The method of claim 49 further comprising providing information to the client using the trusted physical location.

63. The method of claim 62 wherein providing information comprises selecting said information using the trusted physical location.

64. A method comprising:

transmitting first location information from a trusted source within a data network infrastructure;

receiving second location information from a client device requesting access to the network, the second location information using the first location information; and

determining a trusted location using the first and second location information.

65. The method of claim 64 further comprising policing network activities of the client using the trusted physical location.

66. The method of claim 64 further comprising controlling network resources provided to the client using the trusted physical location.

67. A method comprising:

determining a value characterizing a physical location of a device;

determining a level of trust corresponding to the determined value; and

associating the level of trust with the value of the physical location.

68. The method of claim 67 wherein determining a level of trust further comprises determining a level of trust using a precision of a technique used for determining the value of the physical location.

69. The method of claim 67 wherein determining a level of trust further comprises determining a level of trust using a granularity of a range of possible values used for determining the value of the physical location.

70. The method of claim 67 wherein determining a level of trust further comprises determining a level of trust using a probability that determining a value can produce a false value for the physical location.

71. The method of claim 67 wherein determining a level of trust further comprises determining a level of trust using a level of trust of a network device determining the value of the physical location.

72. A system comprising a trusted network device within a data network infrastructure, the network device including a location module configured to determine a trusted physical location of a client device requesting access to the network infrastructure and to associate the trusted physical location with the client device.

73. A method of determining a physical location of a device connected to a data network infrastructure including a plurality of connection points at different physical locations, the method comprising:

measuring a signal characteristic of a communication signal passing via a cable-based transmission medium between a device communicating with the data network infrastructure through one of the connection points; and

determining a physical location of the device according to the measured signal characteristic, including accessing stored information associating signal characteristics with connection points.

74. The method of claim 73 further comprising identifying the connection points with respective connection point identifiers.

75. The method of claim 73 further comprising:

measuring signal characteristics of communication signals passing through each of the plurality of connection points; and

storing information associating each measured signal characteristic and its respective connection point.

76. The method of claim 73 wherein determining a physical location further comprises employing a function that relates values for signal characteristics to respective physical locations.

77. The method of claim 73 wherein the signal characteristics comprise a time delay.

78. The method of claim 73 wherein the signal characteristics comprises at least one of time delay, time-domain reflectometry, signal attenuations, and round-trip delay.

79. A method for surveying a data network infrastructure including a plurality of connection points, the method comprising:

for each of a plurality of connection points each of which provide a cable-based communication path to the data network infrastructure,

determining a signal characteristic for the connection point, and

providing to the network infrastructure the signal characteristic for the connection point.

80. The method of claim 79 further comprising storing an association between each of the connection points and its signal characteristics.

81. The method of claim 79 further comprising identifying each of the connection points with respective connection point identifiers.

82. The method of claim 79 further comprising connecting a location sensing device to a first of the connection points and determining a physical location of said connection point using the location sensing device.

83. The method of claim 82 wherein the location sensing device comprises a GPS receiver.

84. The method of claim 82 further comprising storing an association between the first connection point and its determined physical location.

85. A system comprising:

a transceiver configured to receive an operational signal characteristic from a device communicating with a data network infrastructure through one of a plurality of connection points; and

a location module configured to determine a physical location of the device by comparing the operational signal characteristic with a stored signal characteristic associated with the one connection point.

86. The system of claim 85 wherein the location module is further configured to employ a function that relates values for the signal characteristics to respective physical locations of the connection points.

87. The system of claim 85 wherein the location module further comprises a signal characteristic database having an association of a signal characteristic and its corresponding physical location for each of the connection points.

88. A method comprising:

providing data that includes location-based access control information; and

limiting access to the data at a physical location according to the location-based access control information.

89. The method of claim 88 further comprising determining a physical location of a device accessing the data, and limiting the access according to the determined physical location.

90. The method of claim 88 wherein providing the data includes providing the data in encrypted form, and limiting access to the data includes enabling decryption of the data according to the physical location.

91. The method of claim 88 wherein the data comprises a computer file.

92. The method of claim 91 wherein limiting access to the file includes applying operating system services to limit the access.

93. The method of claim 91 wherein limiting access to the file includes using an application program to limit the access.

94. A method comprising:

receiving data at a device over a data network; and

prohibiting access to that data based on a physical location of the device.

95. A method comprising,

generating data including restrictive routing information based on physical location.

96. The method of claim 95 further comprising transmitting the data in accordance with the restrictive routing information.

97. The method of claim 95 further comprising destroying the data if a network device receiving the data is located at a restricted physical location in accordance with the restricted routing information.

98. The method of claim 95 further comprising prohibiting the data from being transmitted to a network device located at a restricted physical location in accordance with the restricted routing information.

99. The method of claim 95 further comprising prohibiting the data from being accessed by a client device located at a restricted physical location in accordance with the restricted routing information.

100. The method of claim 95 wherein the restricted routing information comprises a prohibited physical location.

101. The method of claim 95 wherein the restricted routing information comprises a permitted physical location.

102. The method of claim 95 wherein the data comprises a data packet.

103. The method of claim 95 wherein the data comprises a file.

104. The method of claim 95 wherein the data comprises a document.

105. A method comprising:
receiving data at a first network device; and
routing the data to a second network device based on a policy determined using location information.

106. A system comprising:
network devices with associated physical locations; and
data with restrictive routing information based on physical location.

107. The system of claim 106 further comprising a physical location server including a storage module configured to store the associations of network devices with their respective physical locations.

108. The system of claim 106 wherein each network device includes a storage module configured to store the association of that particular network device with its respective physical location.

109. The system of claim 106 wherein each network device includes a location module configured to transmit the data in accordance with the restrictive routing information.

110. The system of claim 106 wherein each network device includes a location module configured to destroy the data if the respective network device receiving the data is located at a restricted physical location in accordance with the restricted routing information.

111. The system of claim 106 wherein each network device includes a location module configured to prohibit the data from being transmitted to another network device located at a restricted physical location in accordance with the restricted routing information.

112. The system of claim 106 wherein each network device includes a location module configured to prohibit the data from being accessed by a client device located at a restricted physical location in accordance with the restricted routing information.

113. The system of claim 106 wherein the restricted routing information comprises a prohibited physical location.

114. The system of claim 106 wherein the restricted routing information comprises a permitted physical location.

115. The system of claim 106 wherein the data comprises a data packet.

116. The system of claim 106 wherein the data comprises a file.

117. The system of claim 106 wherein the data comprises a document.

118. Data comprising restrictive routing information based on physical location.

119. The data of claim 118 further comprising a header that includes the restricted routing information.

120. The data of claim 118 wherein the restricted routing information comprises network layer information.

121. The data of claim 118 wherein the restricted routing information comprises transport layer information.

122. The data of claim 118 wherein the restricted routing information identifies prohibited physical locations.

123. The data of claim 118 wherein the restricted routing information identifies permitted physical locations.

124. The data of claim 118 further comprising a data packet.

125. The data of claim 118 further comprising a file.

126. The data of claim 118 further comprising a document.

127. A method comprising:

receiving, at a first device, connection information from a neighboring network device; and

determining a physical location of the first device based on the connection information.

128. The method of claim 127 further comprising receiving, at the first device, the physical location transmitted from the neighboring network device.

129. The method of claim 128 wherein the physical location is a first physical location and the neighboring network device is a first neighboring network device, the method further comprising:

receiving, at the first device, a second physical location transmitted from a second neighboring network device; and

comparing the first physical location with the second physical location to determine a level of confidence of the determined physical location of the first device.

130. The method of claim 128 further comprising associating a level of trust with the physical location based on the neighboring network device.

131. The method of claim 128 wherein the first device belongs to a group consisting of a router, a switch, a network entry device, a firewall device, a gateway, a wireless access point, and a computing device.

132. A system comprising

a location module configured to determine a physical location of a connection point and to transmit the physical location to a client device in communication with the connection point.

133. The system of claim 132 further comprising:

the client device configured to receive the physical location from the physical location module; and

a neighboring network device in communication with the client device, the neighboring network device including the physical location module.

134. The system of claim 133 wherein the physical location is a first physical location and the neighboring network device is a first neighboring network device, the system further comprising:

a second neighboring network device with a physical location module configured to determine a second physical location of the client device and transmit the second physical location to the client device, and

wherein the network device is further configured to receive the second physical location and to compare the first physical location with the second physical location to determine a level of confidence of a physical location of the client device.

135. The system of claim 133 wherein a level of trust, based on the neighboring network device, is associated with the physical location.

136. The system of claim 133 wherein the client device comprises a router, a switch, a network entry device, a firewall device, or a gateway.

137. An article comprising a machine-readable medium that stores executable instruction signals that cause a machine to:

receive, at a first device, connection information from a neighboring network device; and

determine a physical location of the first device based on the connection information.

138. A method comprising,

receiving, at a network entry device of a network infrastructure, a request for network access from a client device;

determining, by the network infrastructure, a physical location of the client device; and determining authorization of the client device based on the physical location.

139. The method of claim 138 wherein determining authorization further comprises determining authorization by the network entry device.

140. The method of claim 138 wherein determining authorization further comprises providing the physical location along with other user credentials to the authorizing device.

141. The method of claim 138 wherein determining authorization further comprises determining a level of service based on the physical location.

142. The method of claim 141 further comprising,

receiving, at the network entry device, user credentials, and

wherein determining authorization further comprises determining a level of service based on the physical location and the user credentials.

143. The method of claim 138 wherein determining authorization further comprises authorizing a user associated with the client device if a level of trust associated with the physical location is not less than a predefined threshold.

144. The method of claim 138 wherein determining authorization further comprising communicating in accord with IEEE 802.1X.

145. A system comprising:

a network infrastructure configured to determine a physical location of a client device, the network infrastructure including:

a network entry device configured to receive a request for network access from a client device and determine authorization of the client device based on the physical location.

146. The system of claim 145 wherein the network entry device is further configured to determine a level of service based on the physical location.

147. The system of claim 145 wherein the network entry device is further configured to receive user credentials and to determine a level of service based on the physical location and the user credentials.

148. The system of claim 145 wherein the network entry device is further configured to authorize a user associated with the client device if a level of trust associated with the physical location is not less than a predefined threshold.

149. The system of claim 145 wherein the network entry device is further configured to communicate in accord with IEEE 802.1X.

150. An article comprising a machine-readable medium that stores executable instruction signals that cause a machine to:

receive, at a network entry device of a network infrastructure, a request for network access from a client device;

determine, by the network infrastructure, a physical location of the client device; and

determine authorization of the client device based on the physical location.

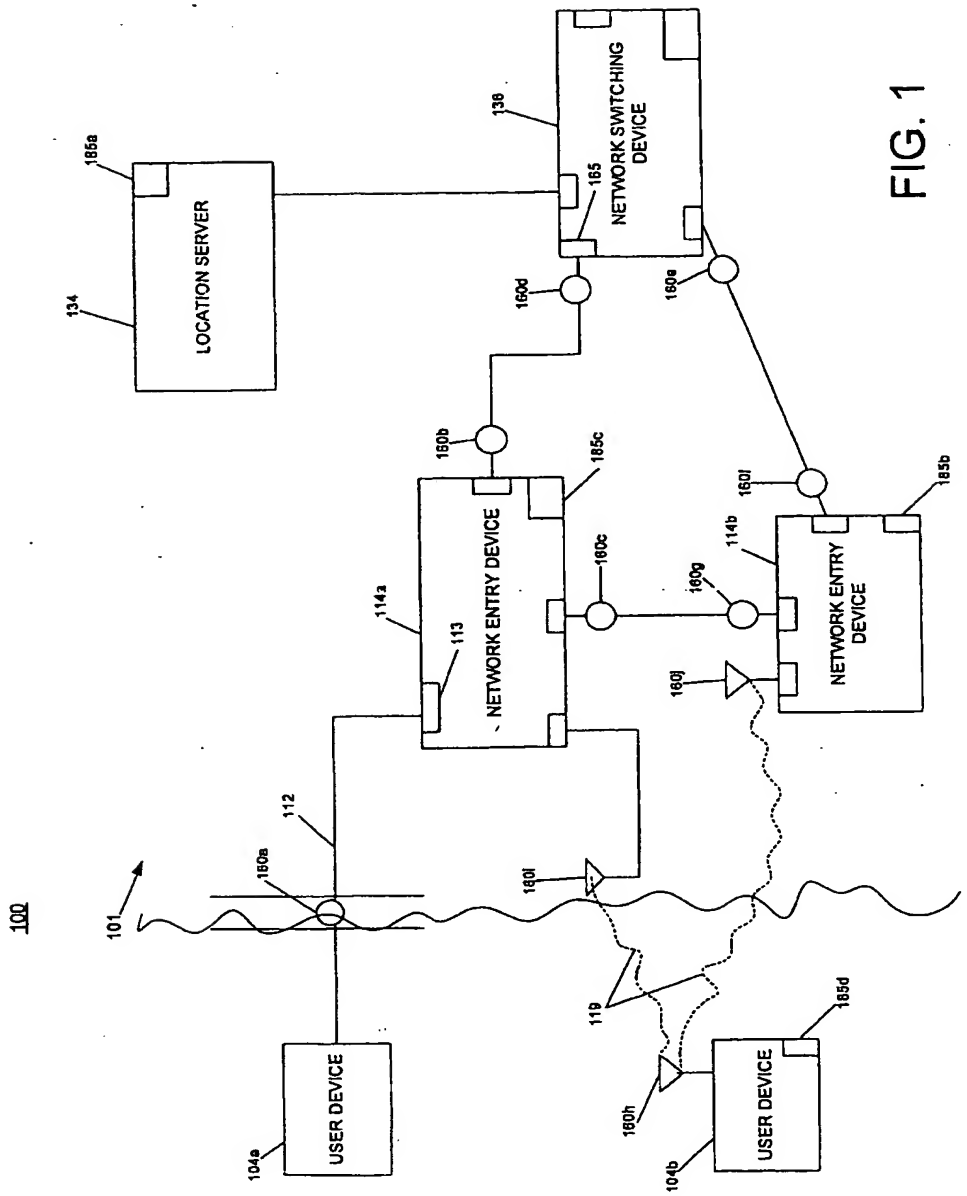

100
101
LOCATION SERVER
134
185a
NETWORK SWITCHING DEVICE
136
165
160d
160a
160b
185c
NETWORK ENTRY DEVICE
114a
113
160c
160g
160l
185b
NETWORK ENTRY DEVICE
114b
160j
112
160a
160l
119
USER DEVICE
104a
160h
185d
USER DEVICE
104b

FIG. 1

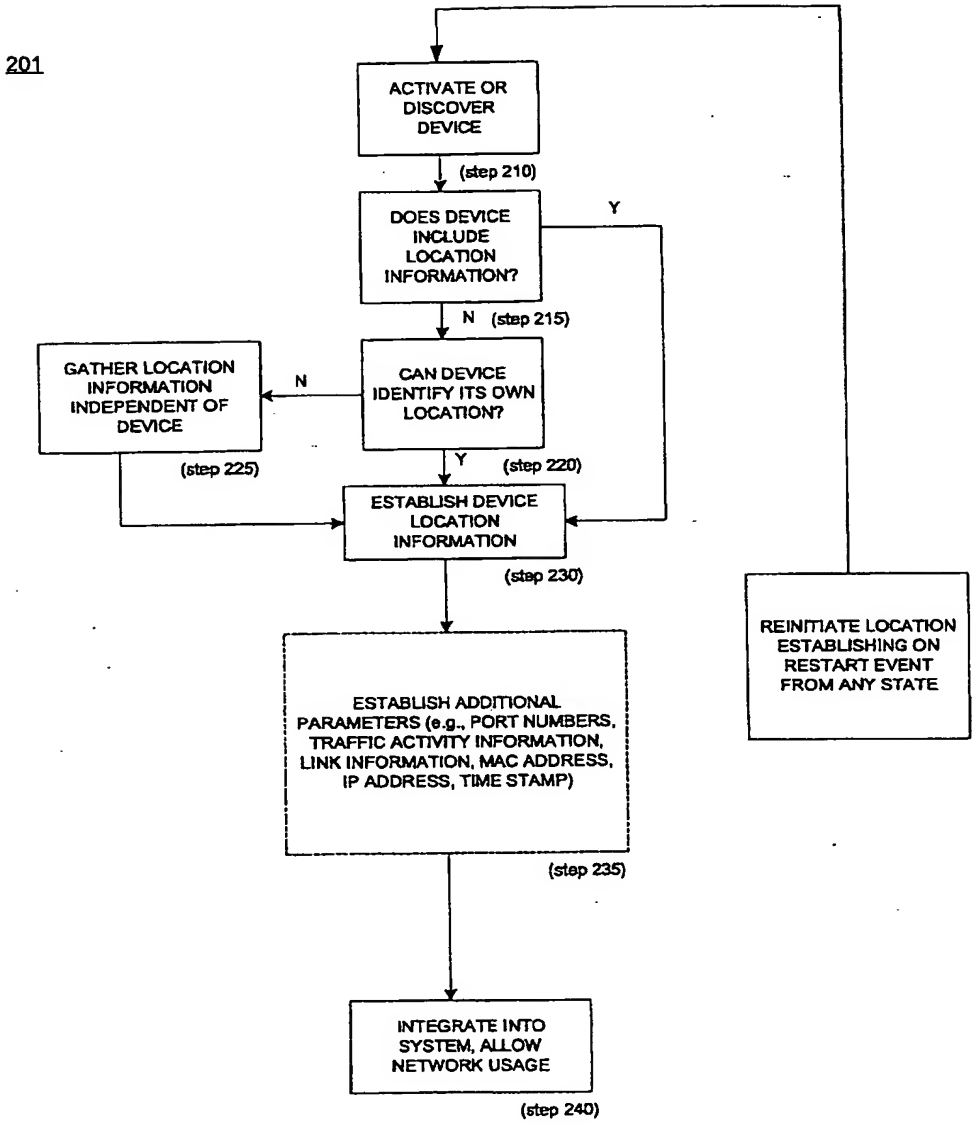

201
ACTIVATE OR DISCOVER DEVICE
(step 210)
DOES DEVICE INCLUDE LOCATION INFORMATION?
Y
N (step 215)
CAN DEVICE IDENTIFY ITS OWN LOCATION?
N
GATHER LOCATION INFORMATION INDEPENDENT OF DEVICE
(step 225)
Y (step 220)
ESTABLISH DEVICE LOCATION INFORMATION
(step 230)
ESTABLISH ADDITIONAL PARAMETERS (e.g., PORT NUMBERS, TRAFFIC ACTIVITY INFORMATION, LINK INFORMATION, MAC ADDRESS, IP ADDRESS, TIME STAMP)
(step 235)
INTEGRATE INTO SYSTEM, ALLOW NETWORK USAGE
(step 240)
REINITIATE LOCATION ESTABLISHING ON RESTART EVENT FROM ANY STATE

FIG. 2

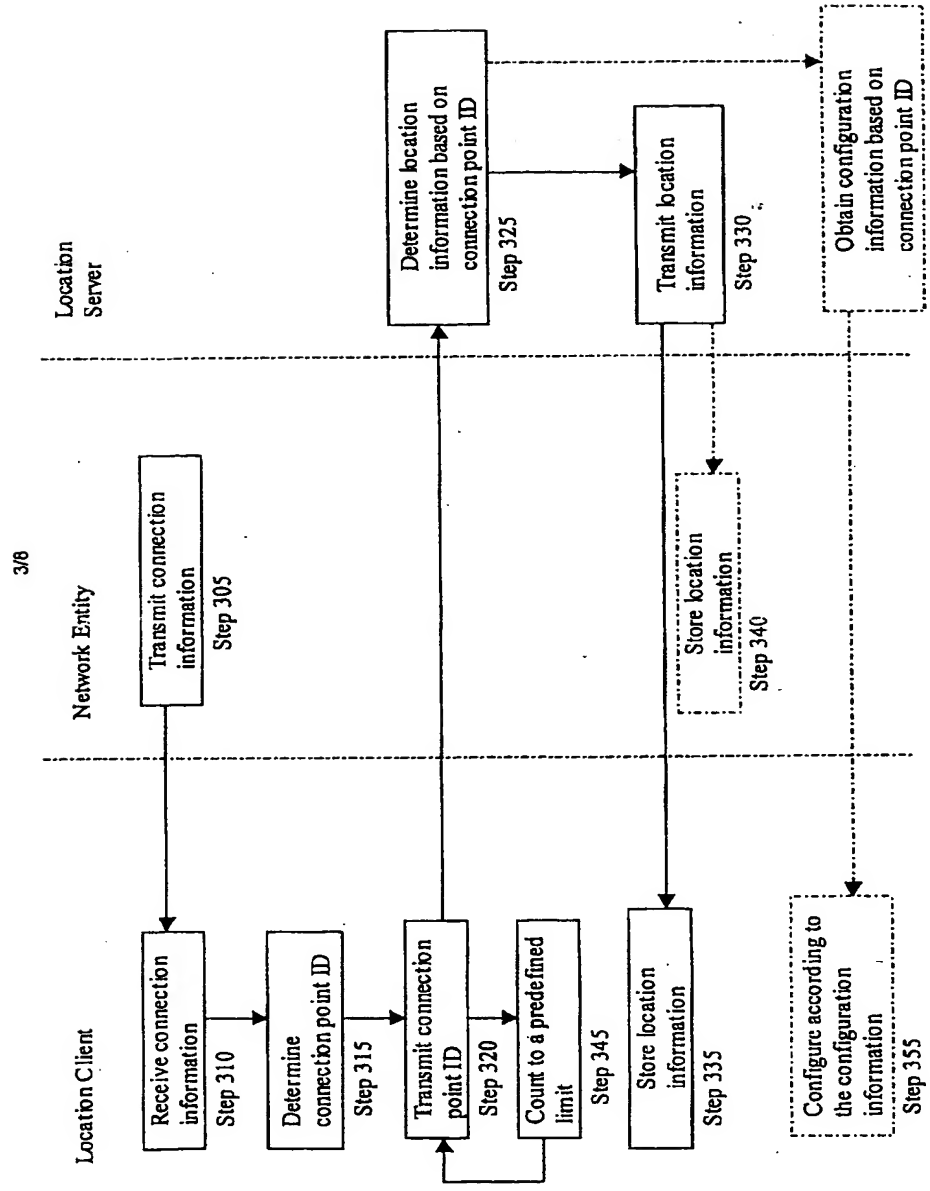

Location Server
Network Entity
Location Client
Transmit connection information
Step 305
Receive connection information
Step 310
Determine connection point ID
Step 315
Transmit connection point ID
Step 320
Count to a predefined limit
Step 345
Determine location information based on connection point ID
Step 325
Transmit location information
Step 330
Store location information
Step 340
Store location information
Step 335
Obtain configuration information based on connection point ID
Step 350
Configure according to the configuration information
Step 355
300

FIG. 3

401

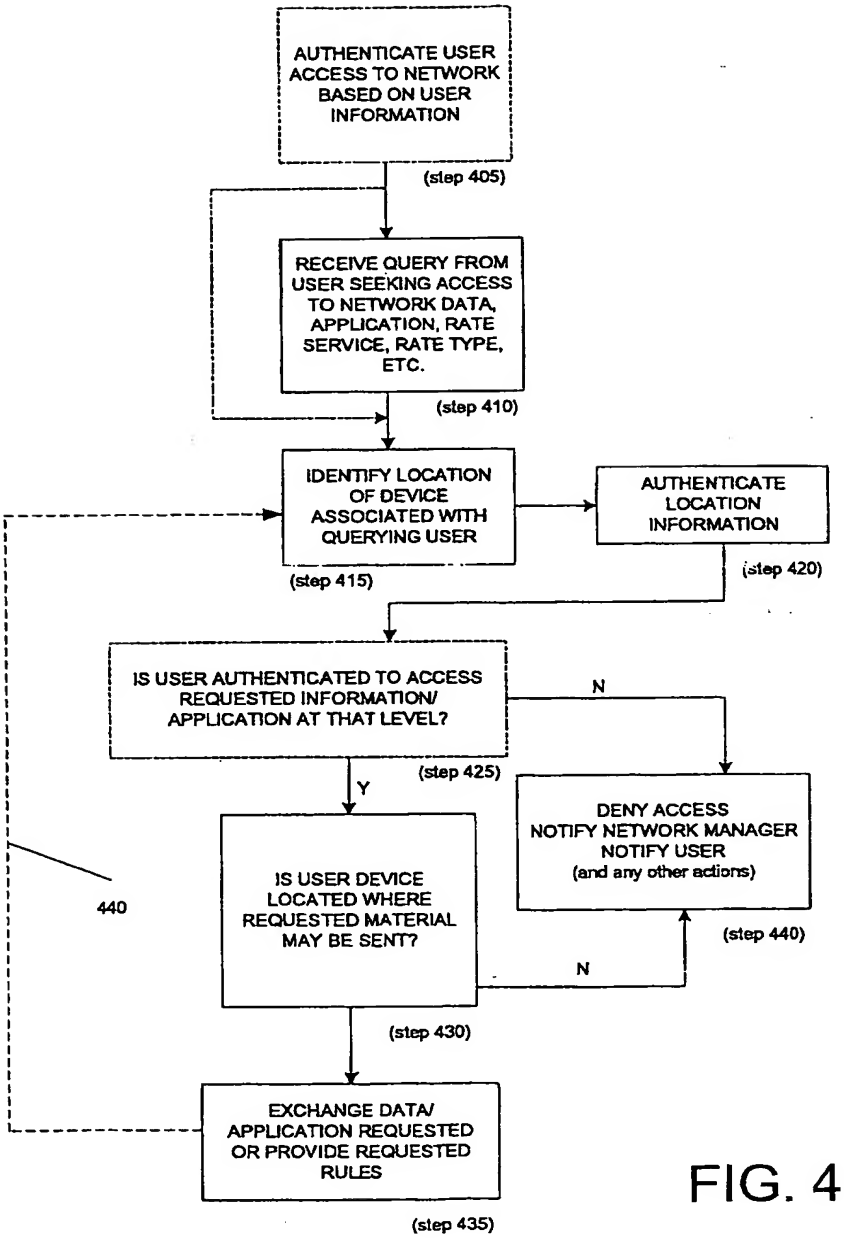

AUTHENTICATE USER ACCESS TO NETWORK BASED ON USER INFORMATION
(step 405)
RECEIVE QUERY FROM USER SEEKING ACCESS TO NETWORK DATA, APPLICATION, RATE SERVICE, RATE TYPE, ETC.
(step 410)
IDENTIFY LOCATION OF DEVICE ASSOCIATED WITH QUERYING USER
(step 415)
AUTHENTICATE LOCATION INFORMATION
(step 420)
IS USER AUTHENTICATED TO ACCESS REQUESTED INFORMATION/ APPLICATION AT THAT LEVEL?
(step 425)
N
Y
DENY ACCESS
NOTIFY NETWORK MANAGER
NOTIFY USER
(and any other actions)
(step 440)
IS USER DEVICE LOCATED WHERE REQUESTED MATERIAL MAY BE SENT?
N
(step 430)
440
EXCHANGE DATA/ APPLICATION REQUESTED OR PROVIDE REQUESTED RULES
(step 435)

FIG. 4

500

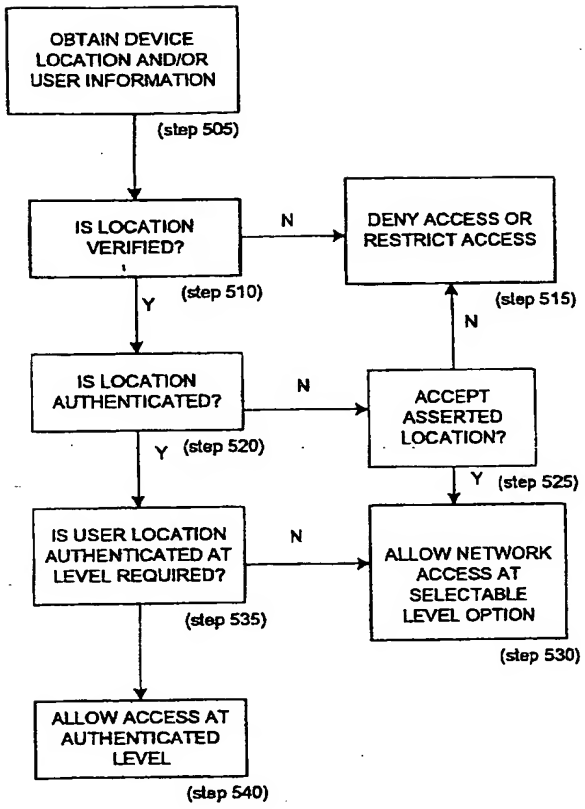

OBTAIN DEVICE LOCATION AND/OR USER INFORMATION
(step 505)
IS LOCATION VERIFIED?
(step 510)
N
DENY ACCESS OR RESTRICT ACCESS
(step 515)
Y
N
IS LOCATION AUTHENTICATED?
(step 520)
N
ACCEPT ASSERTED LOCATION?
Y
(step 525)
Y
IS USER LOCATION AUTHENTICATED AT LEVEL REQUIRED?
(step 535)
N
ALLOW NETWORK ACCESS AT SELECTABLE LEVEL OPTION
(step 530)
ALLOW ACCESS AT AUTHENTICATED LEVEL
(step 540)

FIG. 5

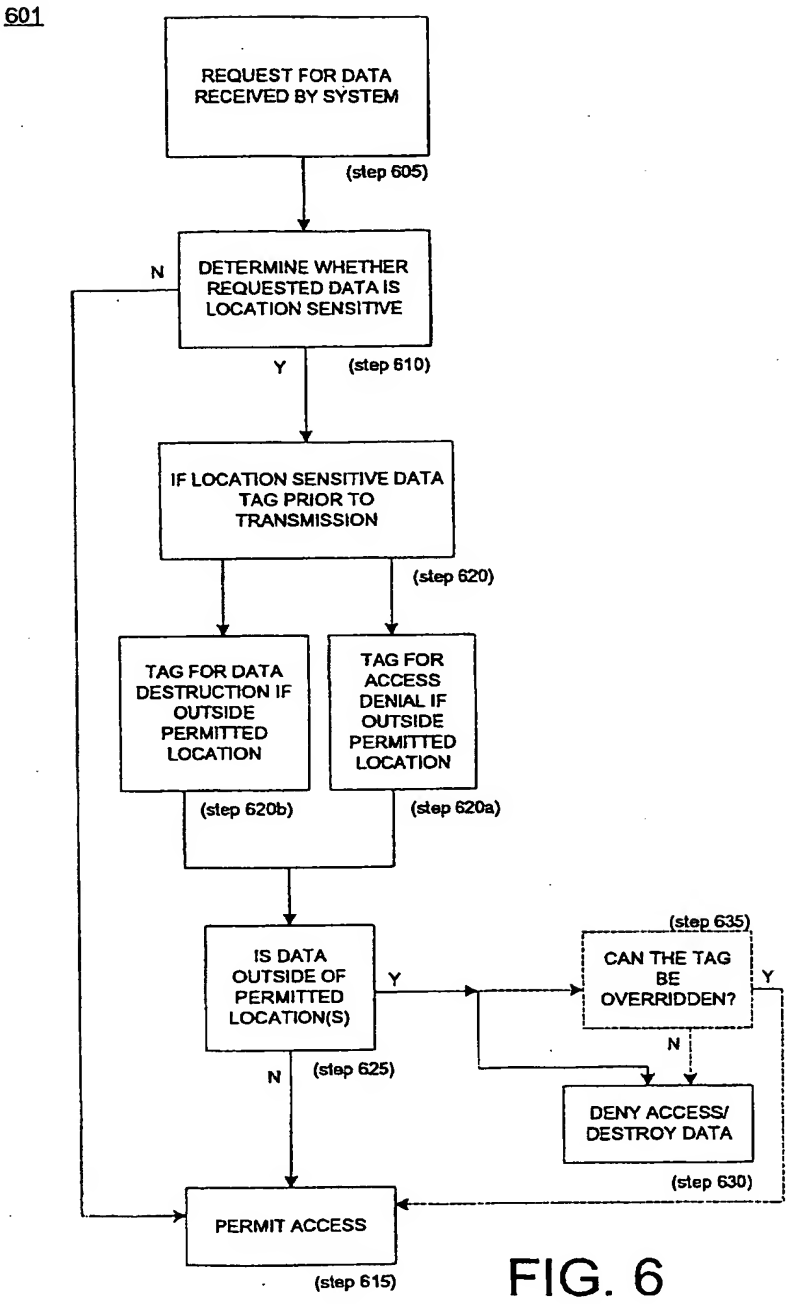

601
REQUEST FOR DATA RECEIVED BY SYSTEM
(step 605)
DETERMINE WHETHER REQUESTED DATA IS LOCATION SENSITIVE
N
Y
(step 610)
IF LOCATION SENSITIVE DATA TAG PRIOR TO TRANSMISSION
(step 620)
TAG FOR DATA DESTRUCTION IF OUTSIDE PERMITTED LOCATION
(step 620b)
TAG FOR ACCESS DENIAL IF OUTSIDE PERMITTED LOCATION
(step 620a)
IS DATA OUTSIDE OF PERMITTED LOCATION(S)
Y
N
(step 625)
(step 635)
CAN THE TAG BE OVERRIDDEN?
Y
N
DENY ACCESS/ DESTROY DATA
(step 630)
PERMIT ACCESS
(step 615)

FIG. 6

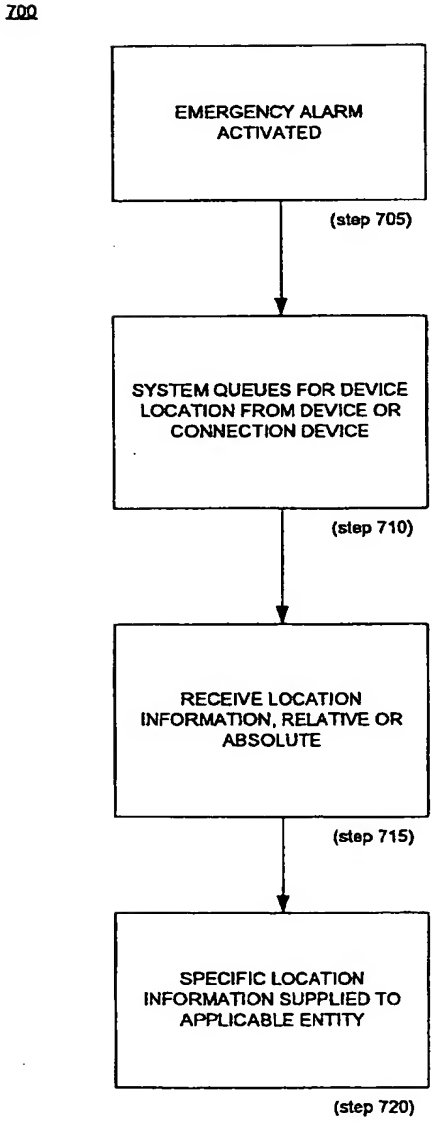

700
EMERGENCY ALARM ACTIVATED
(step 705)
SYSTEM QUEUES FOR DEVICE LOCATION FROM DEVICE OR CONNECTION DEVICE
(step 710)
RECEIVE LOCATION INFORMATION, RELATIVE OR ABSOLUTE
(step 715)
SPECIFIC LOCATION INFORMATION SUPPLIED TO APPLICABLE ENTITY
(step 720)

FIG. 7

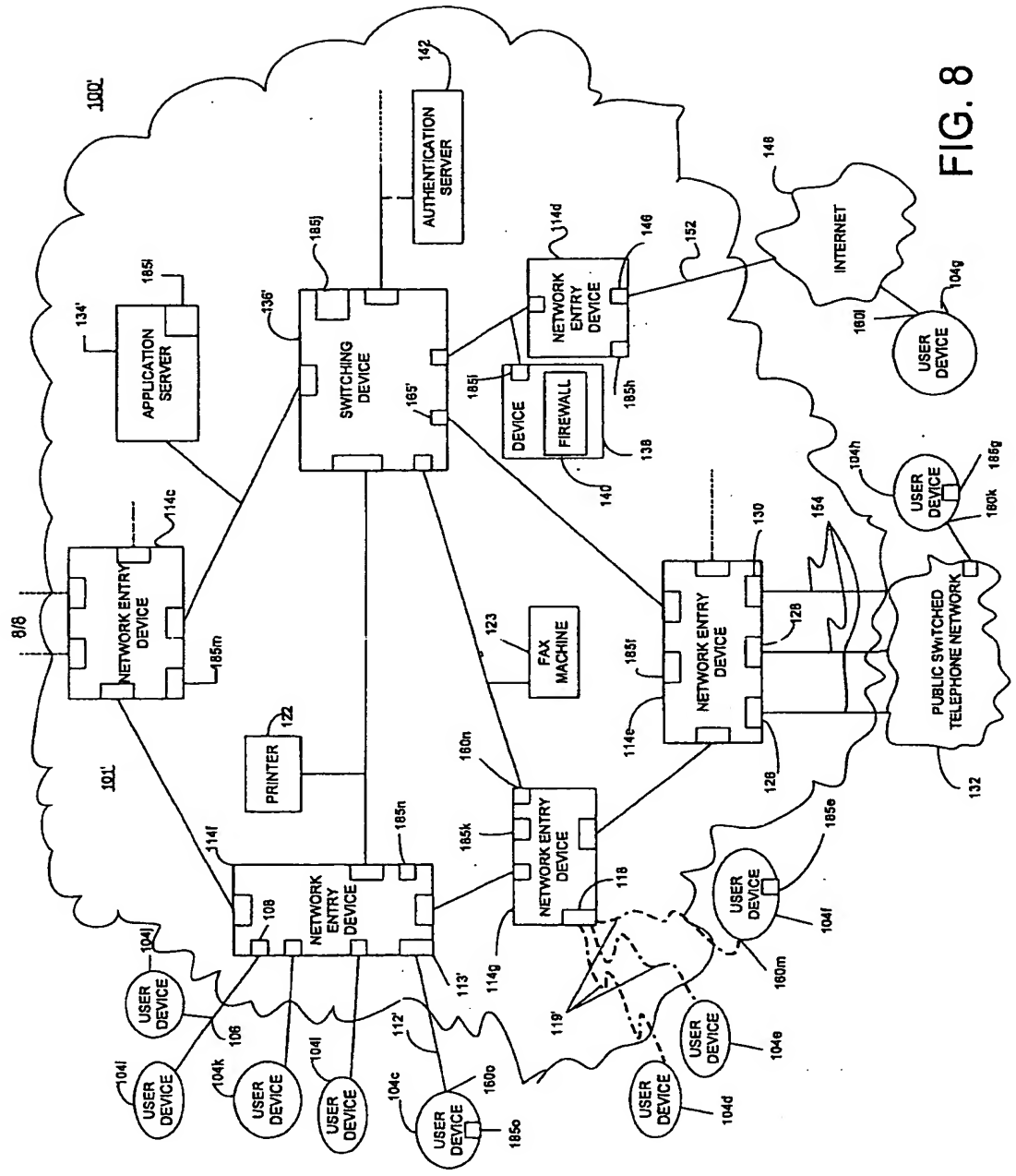

100'
101'
AUTHENTICATION SERVER
142
APPLICATION SERVER
134'
SWITCHING DEVICE
136'
NETWORK ENTRY DEVICE
114d
INTERNET
148
DEVICE
FIREWALL
138
140
USER DEVICE
104g
160l
NETWORK ENTRY DEVICE
114c
NETWORK ENTRY DEVICE
130
PUBLIC SWITCHED TELEPHONE NETWORK
132
FAX MACHINE
123
PRINTER
122
NETWORK ENTRY DEVICE
114f
NETWORK ENTRY DEVICE
118
NETWORK ENTRY DEVICE
114g
USER DEVICE
104l
USER DEVICE
104k
USER DEVICE
104i
USER DEVICE
104c
USER DEVICE
104d
USER DEVICE
104e
USER DEVICE
104f
USER DEVICE
104h
8/8

FIG. 8